Department of the Army
Technical Architecture

Version 4.0

30 January 1996

This page was intentionally left blank.

INTERNET AVAILABILITY

This document is available electronically on the World Wide Web (WWW) at Uniform Resource Locator (URL) "http://www.hqda.army.mil/webs/techarch/". The electronic version contains “HotLinks” to many of the referenced standards.

COMMENTS ON THE ARMY TECHNICAL ARCHITECTURE

To speed processing and consideration, comments and suggested changes should be submitted electronically via Email. Comments submitted as attached word processing documents should be in either Microsoft Word 6.0 or WordPerfect 5.2 format.

Send Email comments to “techarch@www.hqda.army.mil”.

This is where all comments are received and logged in. A reference number will be assigned and we will send you an acknowledgment of your comment. The comment will be forwarded to all workgroups that should address your comment. Receiving comments by Email allows us to rapidly address your comment in the appropriate workgroup(s) and make the necessary changes in the next revision.

Your comment should include the following information: name, organization, phone number, recommended change including section number, and reason. Comments should be as specific as possible, referencing a specific standard or section and providing recommended changes with a brief justification for each change.

More information and an example can be found on the WWW at URL "http://www.hqda.army.mil/webs/techarch/faq.htm".

TRADEMARKS AND REFERENCES

Trademarked names appear throughout this document. Rather than list the names and entities that own the trademarks or insert a trademark symbol with each mention of the trademarked name, the publisher states that it is using the names only for editorial purposes and to the benefit of the trademark owner with no intention of infringing upon that trademark.

Appendix B contains a list of references that provide the full citation for each reference found in the document.

This page was intentionally left blank.

TABLE OF CONTENTS

SECTION **PAGE**

SECTION 1

TECHNICAL ARCHITECTURE OVERVIEW

1.1 INTRODUCTION

1.1.1 Purpose

The Army's Technical Architecture (ATA) has three mutually supporting objectives. First and foremost, to provide the foundation for a seamless flow of information and interoperability among all tactical, strategic, and sustaining base systems that produce, use, or exchange information electronically. Second, to provide guidelines and standards for system development and acquisition that will dramatically reduce cost, development time, and fielding time for improved systems. Third, to influence the direction of the information industry's technology development and research & development investment so that it can be more readily leveraged in Army systems.

This section provides an overview of the ATA. It describes the purpose, scope, and background of the ATA, what is new in this version and what is covered by each section.

1.1.2 Architectures Defined

Recent years have seen a proliferation of "architectures" within the Department of Defense (DOD) Command, Control, Communications, and Computers (C4) and Information System communities. In a study during the Summer of 1994, the Army Science Board (ASB) defined an interrelated set of architectures: Operational, Systems, and Technical. These concepts have been adopted not only by the Army in its Enterprise Strategy, but by the other Services and DOD as well. Figure 1-1 shows the relationship among the three architectures. The definitions are provided here to ensure a common understanding of the different types of architectures and how the ATA fits into the overall scheme.

1.1.2.1 Technical Architecture

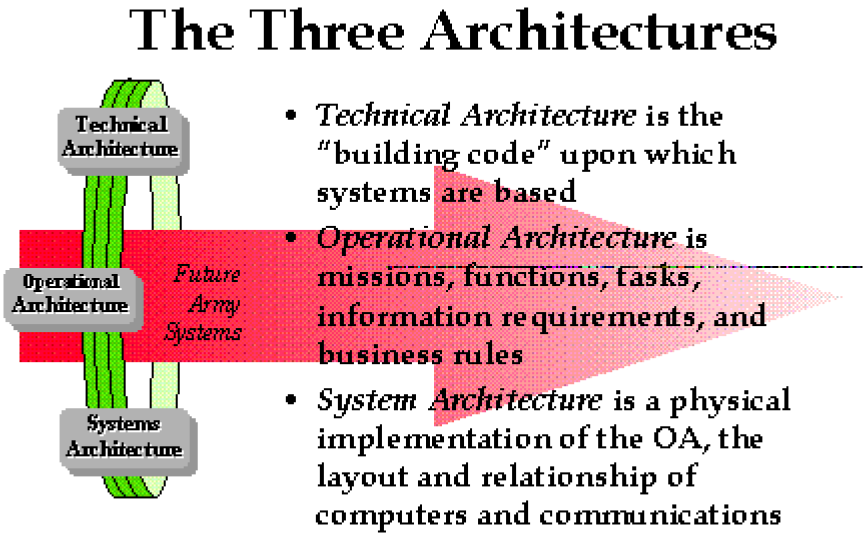
A **Technical Architecture** (TA) is the minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements that together may be used to form an information system. Its purpose is to ensure that a conformant system satisfies a specified set of requirements. It is the building code for the Systems Architecture being constructed to satisfy Operational Architecture requirements. (C4I Service Chiefs Warrior Focused Definitions, Jan 96)

1.1.2.2 Operational Architecture

An **Operational Architecture** (OA) is a description, often graphical, which defines the force elements and the requirement to exchange information between these force elements. It defines the types of information, the frequency of its exchange, and what warfighting tasks are supported by these information exchanges. It specifies what the information systems are operationally required to do and where these operations are to be performed. (C4I Service Chiefs Warrior Focused Definitions, Jan 96)

1.1.2.3 Systems Architecture

A **Systems Architecture** (SA) is a description, often graphical, of the systems solution used to satisfy the warfighter's Operational Architecture requirement. It defines the physical connection, location, and identification of nodes, radios, terminals, etc., associated with information exchange. It also specifies the system performance parameters. The Systems Architecture is constructed to satisfy Operational Architecture requirements per the standards defined in the Technical Architecture. (C4I Service Chiefs Warrior Focused Definitions, Jan 96)



The Three Architectures

- *Technical Architecture* is the "building code" upon which systems are based
- *Operational Architecture* is missions, functions, tasks, information requirements, and business rules
- *System Architecture* is a physical implementation of the OA, the layout and relationship of computers and communications

FIGURE 1-1. THE DIFFERENT ARCHITECTURES

1.1.3 Scope

The ATA applies to all systems that produce, use, or exchange information electronically. The ATA will be used by anyone involved in the management, development or acquisition of new or improved systems. Within the Army, the Vice Chief of Staff, Army and the Army Acquisition Executive have jointly made each Milestone Decision Authority (MDA), Major Army Command (MACOM), Program Executive Officer (PEO), Program or Product Manager (PM), Advanced Technology

Demonstration (ATD) Manager, Advanced Concept and Technology Demonstration (ACTD) Manager and Advanced Concept and Technology (ACT) II Manager responsible for compliance with this ATA. System developers will comply with the ATA in order to ensure that products meet interoperability, performance, and sustainment criteria. Combat developers will use the ATA in developing requirements and functional descriptions. Battle Labs will use the ATA to ensure that the fielding of their "good ideas" is not unduly delayed by the cost and time required for wholesale reengineering to meet interoperability standards.

Expanding the scope and the focus of Version 3.1 of the ATA requires more than adding standards for weapons and sustaining base systems. It requires a qualitative growth in perspective. In order to fully achieve the Force XXI vision of total, seamless integration and synchronization of military power, the Army must achieve and maintain interoperability across a continuum of several dimensions at once:

- Among battlefield weapons systems, sensors and shooters -- tanks, aircraft, UAVs;
- Among C3I and Support systems;
- Along the vertical and horizontal dimensions of organizational and command structures;
- Across the Joint dimension among Army, Air Force, Navy, USMC, JCS/CINC, & DISA at the lowest practical echelon;
- Across the power projection dimension - from the sustaining base forward to the Company Command Post;
- Across the time and technology generation dimension - to achieve backward and forward compatibility and interoperability.

Compliance is enumerated in an implementation/migration plan. A system is compliant with the ATA if it meets, or is implementing an approved plan to meet, all applicable ATA mandates. In practical terms, progress toward compliance is assessed through a migration strategy and a planning process that considers a host of resource, management, and operational issues that affect overall system development and determine the best approach for satisfying a validated user need.

1.1.4 Background

The evolution of national military strategy in the post cold war era and the economic reality of a shrinking budget have resulted in a new vision for the Department of Defense. This vision is most commonly known as *C4I for the Warrior*. It recognized an increased reliance on information systems to provide the decisive edge in combat. The associated Service visions are articulated in the following documents: The Army Strategy: *The Enterprise Vision*; The Air Force Strategy: *Horizon*; The Navy Strategy: *Copernicus…Forward*; and the Marine Strategy: *MAGTF/C4I.*

To achieve the principles outlined in *The Army Enterprise Vision*, the Army developed and published the *Army Enterprise Implementation Plan.* This plan provided a blueprint for migration, directed tasks to implement *The Vision*, and provided a management structure. One of the tasks of the implementation plan was that a Technical Architecture be established to support the seamless sharing of information on a worldwide basis. The plan directed the Office of the Director of Information Systems for C4 (ODISC4) to develop and implement an Army Technical Architecture, with the support of various organizations. The relationship of the ATA to DOD and other Service Architectures is shown in Figure 1-2.

The ATA follows an azimuth set by the DOD. On 13 October 1993, the DOD issued a memorandum that included guidance for the incorporation of "interoperability, technical integration, DOD standard data, and integrated databases to provide higher quality and lower cost information technology services for all users." This memorandum further stated that "Integration implies seamless, transparent operation of DOD systems based on a shared or commonly-derived architecture (functional or technical) and standard data." On 29 June 1994, the DOD reinforced this change in direction through a memorandum calling for " the use of performance and commercial specifications and standards in lieu of military specifications and standards, unless no practical alternative exists". The ATA is fully responsive to these mandates.

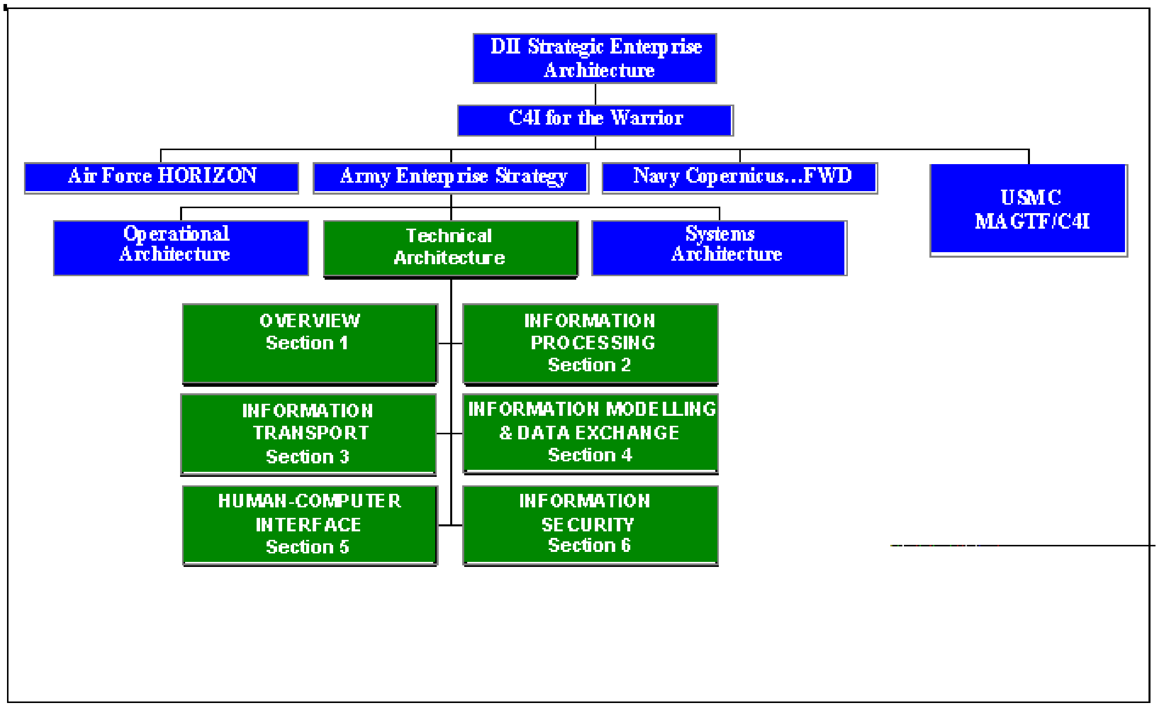

DII Strategic Enterprise Architecture
C4I for the Warrior
Air Force HORIZON
Army Enterprise Strategy
Navy Copernicus...FWD
USMC MAGTF/C4I
Operational Architecture
Technical Architecture
Systems Architecture
OVERVIEW Section 1
INFORMATION PROCESSING Section 2
INFORMATION TRANSPORT Section 3
INFORMATION MODELLING & DATA EXCHANGE Section 4
HUMAN-COMPUTER INTERFACE Section 5
INFORMATION SECURITY Section 6

FIGURE 1-2. DOCUMENT TREE

Version 3.1 of the Army Technical Architecture was published 31 March 1995. This version was mandated for use by the Army Acquisition Community with a requirement to provide a plan for migrating all systems to conform to the mandated standards. Results from a review of many of these plans, plus numerous comments from the field, provided the basis for this new version, 4.0. This version incorporates improvements as well as expands the scope to address Weapons Systems, Sustaining

Base systems, and Information Security. Since information exchanged between weapons systems often travels via C3I systems, the standards in Version 3.1 of the TA remain the core and baseline of the expanded ATA. In order to be more discriminating in the applicability of standards and to extend the ATA without complicating the base document, this version adds appendices for each of four focus areas or "domains" - Sustaining Base & Office Automation, C3I, Weapons, and Modeling & Simulation.

1.1.5 Basis for the ATA

The ATA is based on four primary sources: (1) acquisition reform initiatives such as the mandate to use widely accepted commercial standards; (2) standards used in existing Army systems; (3) the Defense Information Infrastructure (DII) Strategic Enterprise Architecture (SEA) and Common Operating Environment (COE); and (4) guidance provided by the DOD's Technical Architecture Framework for Information Management (TAFIM), Version 2.0.

> NOTE: The TAFIM 3.0, DII SEA (Coordinating Draft 31 May 95), and GCCS/DII COE Specifications were only available in draft form during the development of this version of the ATA. When these documents are available in final approved form, the ATA will be adjusted as necessary.

The TAFIM provides a technical architecture definition that documents the services, standards, design concepts, components, and configurations that can be used to guide the development of technical architectures. The key portion of the TAFIM is Volume 2, the Technical Reference Model (TRM), which identifies a target framework and set of standards for the DOD computing and communications infrastructure. The underlying premise of the TRM is the implementation of an open systems environment. This environment allows information systems to be developed, operated, and maintained, independent of applications or proprietary vendor products. The TAFIM uses Commercial, Federal, National, and International standards, which are adopted by industry, and standards that are agreed to by the U.S. and its allies, as well as DOD standards. By implementing well defined, widely known, commercially popular, and consensus-based standards, the Army can leverage the commercial marketplace's investments and ensure a migration path into the future.

1.1.6 What's New in This Version

- Expansion of scope from C4I domain to encompass ALL Army systems and programs that produce, use, or exchange information electronically.
- Addition of Section on Information Security.
- Replaced MIL STDs with equivalent commercial standards where feasible.
- Updated referenced standards to current approved versions.
- Where standards have sufficiently matured they have been moved from*emerging* to *mandated* status.

- Updated to reflect updated versions of foundation documents such as TAFIM, published GCCS/DII COE specifications, and DII SEA.

1.2 TECHNICAL ARCHITECTURE

The technical direction within this document represents the implementation of the 1994 ASB recommendations to develop a strong, enforceable technical architecture with a heavy emphasis on commercial standards and profiles. The intent is to achieve interoperability while reducing cost, by leveraging the large investment industry has made in developing and implementing standards-based technologies that are in widespread use. Every effort has been made to avoid closed commercial or military-unique standards. The standards contained herein are based primarily on commercial "open systems" technologies that are being adopted by the joint community. Military standards are used only where absolutely necessary. A hierarchy of standards by family was developed to guide selection of specific standards for incorporation in this version of the ATA. The general order of preference, subject to modifications due to specific operational interoperability requirements and acceptance in the commercial marketplace, favored standards specified by neutral standard groups such as IEEE or ISO, followed by industry consortiums such as the Open Systems Foundation, then vendor standards that are so widely supported as to be de facto industry standards, and finally government standards such as FIPS and MIL STDs.

NOTE: Many of the Government standards specified in the ATA are actually a profile of a commercial standard. A profile amplifies but does not modify the basic standard; that is, it specifies values for parameters or options, or it clarifies implementation details. All non-commercial standards mandated in the ATA have met the requirements of the DOD Commercial Standards Policy and can be used without any additional requests for waiver or exception to policy.

1.2.1 COMMON OPERATING ENVIRONMENT/ DOMAINS

An increasing amount of Army system development effort is spent in developing and testing computer software. In addition, even when software development is completed on schedule, few systems these days operate in isolation, so an additional amount of time and effort must be spent on maintaining specialized interfaces to external systems that are themselves changing over time. To alleviate this problem the concept of a Common Operating Environment (COE) was developed. It is a powerful mechanism that standardizes the external environment interface and the Application Program Interface (API) for a mission application system developer and maintains interoperability over time because the common software substrate is upgraded as a whole. It also frees the mission application developer to concentrate efforts on enhancing operational functionality rather than building common services.

DOD has adopted the COE concept in the DII COE, with its first implementation being the Global Command and Control System (GCCS) COE, which was referenced for use in Version 3.1 of the Army TA. This COE lays the foundation for the provision of standardized, common services and is described as a software architecture, an approach for building interoperable systems, a collection of reusable software components, a software infrastructure, and a set of guidelines and standards. The main emphasis in this version of the ATA is utilizing the COE concept, software architecture, and building to a standard layer of APIs.

Studies of software reuse in Army and DOD systems indicate that the largest potential for reusing mission application software and process models is within a domain where functions and methods are the same. To better facilitate mission-application software reuse, a structure of domains, or common focus areas, are shown in Figure 1-3.

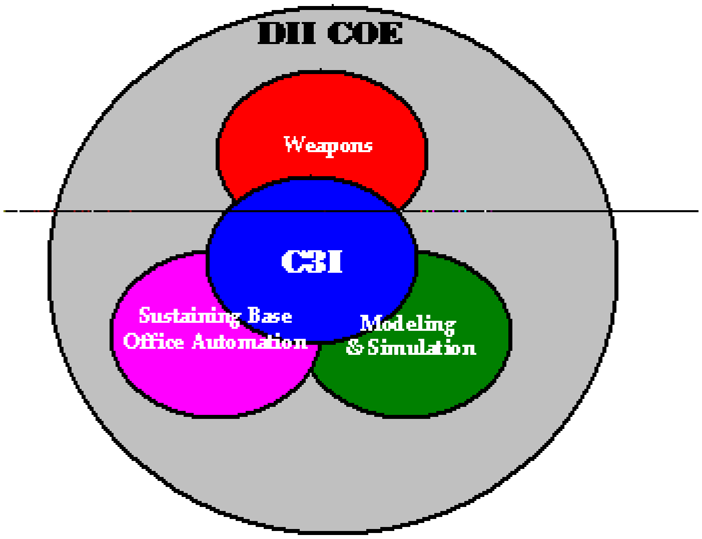


FIGURE 1-3 ARMY SYSTEM DOMAINS

There is only one DII COE concept, process, and approach. However, one specific COE implementation of software components and infrastructure cannot satisfy the requirements of all systems. The ATA envisions the tailoring of software components and infrastructure within a hierarchy of implementations of the COE, starting with high level domains, with specialized component sets tailored for each common area. In this way, common reusable software and products are inherited downward and either used as is, or replaced or augmented with more specialized software modules.

1.2.2 DOCUMENT ORGANIZATION

This document consists of six sections: (1) Overview; (2) Information Processing Standards; (3) Information Transport Standards; (4) Information Modeling and Data Exchange Standards; (5) Human-Computer Interfaces; and (6) Information Security. These sections provide the core standards which apply to all systems.

In addition, there is an appendix for each domain containing exceptions (replace a core standard with a domain standard) or extensions (add a domain standard in addition to a core standard).

- Appendix D - Sustaining Base & Office Automation.
- Appendix E - C3I.
- Appendix F - Weapons.
- Appendix G - Modeling and Simulation.

Each section, except for the overview, is divided into three subsections as follows:

- *Introduction* - This subsection is for information only. It provides background descriptions and definitions that are unique to the section.
- *Mandates* - This subsection contains the mandatory standards (and profiles) within the section. Mandatory standards shall be implemented by systems that have a need for the corresponding interoperability-related services. **A standard is mandatory in the sense that if a service is going to be implemented, it shall be implemented in accordance with the associated ATA standard.**If a service is provided by more than one standard (e.g., local area network standards), the appropriate standard should be selected based on system requirements. Many standards have optional parts, or parameters that can affect interoperability. In those cases a commercial standard may be further modified by a standard profile to ensure proper operation.
- *Emerging Standards* - This subsection provides guidance for designing "forward compatibility" into systems. It lists standards that are not yet mandatory, but that probably will be adopted in the near future. The expectation is that emerging standards will be elevated to mandatory status when commercial implementations of the standards mature. System developers must design with an eye to these emerging standards so that they can be readily incorporated into future upgrades.

1.2.2.1 Information Processing Standards

Section 2 mandates government and commercial information processing standards the Army will use to develop integrated, interoperable systems that meet the warfighter's information processing requirements. This section also describes the Common Operating Environment (COE) concept and individual processing standards.

1.2.2.2 Information Transport Standards

Section 3 describes the information transport standards and profiles that are essential for information transport interoperability and seamless communications. This section mandates the use of the open-systems standards used for the Internet and the Defense Information Systems Network (DISN). These networks use the Internet Protocol (IP) suite, which provides communications interoperability between systems that are on different platforms or communications networks.

1.2.2.3 Information Modeling and Data Exchange Standards

Section 4 mandates the use of integrated information modeling to define functional and information requirements. Information modeling consists of IDEF0 process modeling and IDEF1X data modeling. The DOD Enterprise Model forms the overall framework for development and/or extension of process models for specific programs. The role of the DOD C2 Core Data Model and the Defense Data Dictionary System (DDDS), formerly the Defense Data Repository System (DDRS), are explained. The section describes the use of existing standard messages as an interim solution until mechanisms for the exchange of standard data elements are finalized.

1.2.2.4 Human-Computer Interfaces

Section 5 provides a common framework for Human-Computer Interface (HCI) design and implementation in Army automated systems. The objective is the standardization of user interface implementation options, enabling Army applications to appear and behave in a reasonably consistent manner. The section specifies HCI design guidance, mandates, and standards. The standardization of HCI appearance and behavior within the Army will result in higher productivity, shorter training time, and reduced development costs.

1.2.2.5 Information Security

The determination of security services to be used and their strength is one primary aspect of developing the security policy for an information domain or system. The choices made are dependent on policy, threats, vulnerabilities, and acceptable risk. This determination is an operational decision and is beyond the scope of the ATA. However, once the determination is made of which security services are needed, their strength, and at what system level to best provide each service, this section prescribes what standards and protocols are used to satisfy security requirements, maintain interoperability, and reduce cost through reuse. It is an interim supplement to Volume VI of the TAFIM until such time as the DOD Goal Security Architecture (DGSA) is implemented.

To be effective, security standards must be integrated into and used with the other information standards in the ATA. Therefore this section is structured to shadow the overall organization of the ATA in order that readers can easily link security topics with the related subject area in the core sections of the ATA.

This page was intentionally left blank.

SECTION 2

INFORMATION PROCESSING STANDARDS

2.1 INTRODUCTION

2.1.1 Purpose

The purpose of this section is to specify the ATA information processing standards the Army will use to develop integrated, interoperable systems that directly or indirectly support the warfighter.

Information processing standards support the objectives of reducing cost and time of development, easing software integration and maintenance, and improving interoperability. The primary mechanism is the *concept* of a Common Operating Environment (COE) that provides a reusable set of common software services via standard application programming interfaces (APIs). By building modular applications that use a common software infrastructure accessed through a stable set of APIs, developers should be able to "plug and play" their applications into a centrally maintained infrastructure. The use of the standard APIs allows the COE and mission applications to be quickly integrated and updated relatively independent of each other. The COE concept allows developers to concentrate their efforts on building mission area applications rather than building duplicative system service infrastructure software. Common standards such as SQL to communicate with relational database management systems and Computer Graphics Metafile (CGM) to store graphics support the objective of interoperability. Systems developed to these standards should be able to share services (retrieve authorized data from each others databases) and data (such as an overlay). The use and evolution of the COE concept and the ATA standards it embodies, will advance the goal of building systems that are compatible while minimizing program costs through systematic software reuse. The Army software reuse policy is defined in the Army Reuse Policy document.

2.1.2 Scope

This section applies to mission area, support application, and application platform service software developed or procured by the Army that process information for systems specified in paragraph 1.1.3. This section does not cover communications standards needed to transport information between systems (refer to Section 3), nor standards relating to information modeling (process, data, and simulation), data elements, or military unique message set formats (refer to Section 4).

2.1.3 Background

The COE Concept is described in Section 1. It is implemented with a set of modular software that provides generic functions or services such as operating system services. These services or functions are accessed by other software through standard APIs. The DII COE may have to be adapted and tailored to meet the specific requirements of a domain. The key is that domain implementations adhere to the COE concept in that they provide standard modularized software services that are consistent with the TAFIM TRM and that application programmers have access to these services through standard APIs.

The individual standards contained in this section and applicable appendices that will be used to implement a domain COE are presented within the framework of the TAFIM TRM. This reference model was intentionally generalized and does not imply any specific system architecture. Its purpose is to provide a "set of concepts, entities, interfaces, and diagrams that provides a basis for the specification of standards." The TAFIM TRM organizes software into two entities, an Application Software Entity and an Application Platform Entity. The Application Software Entity communicates with the Application Platform Entity through an API. The Application Platform Entity communicates with the external environment through the External Environment Interface (EEI). The TAFIM TRM decomposes these entities into subcategorizes as shown in Figure 2-1. The application software entity and associated mandates are detailed in Section 2.2.1 while the Application Platform's seven major service areas and associated mandates are detailed in Section 2.2.2.1 . Section 2.2.2.2 defines the Application Platform Cross-Area Services and their associated mandates.

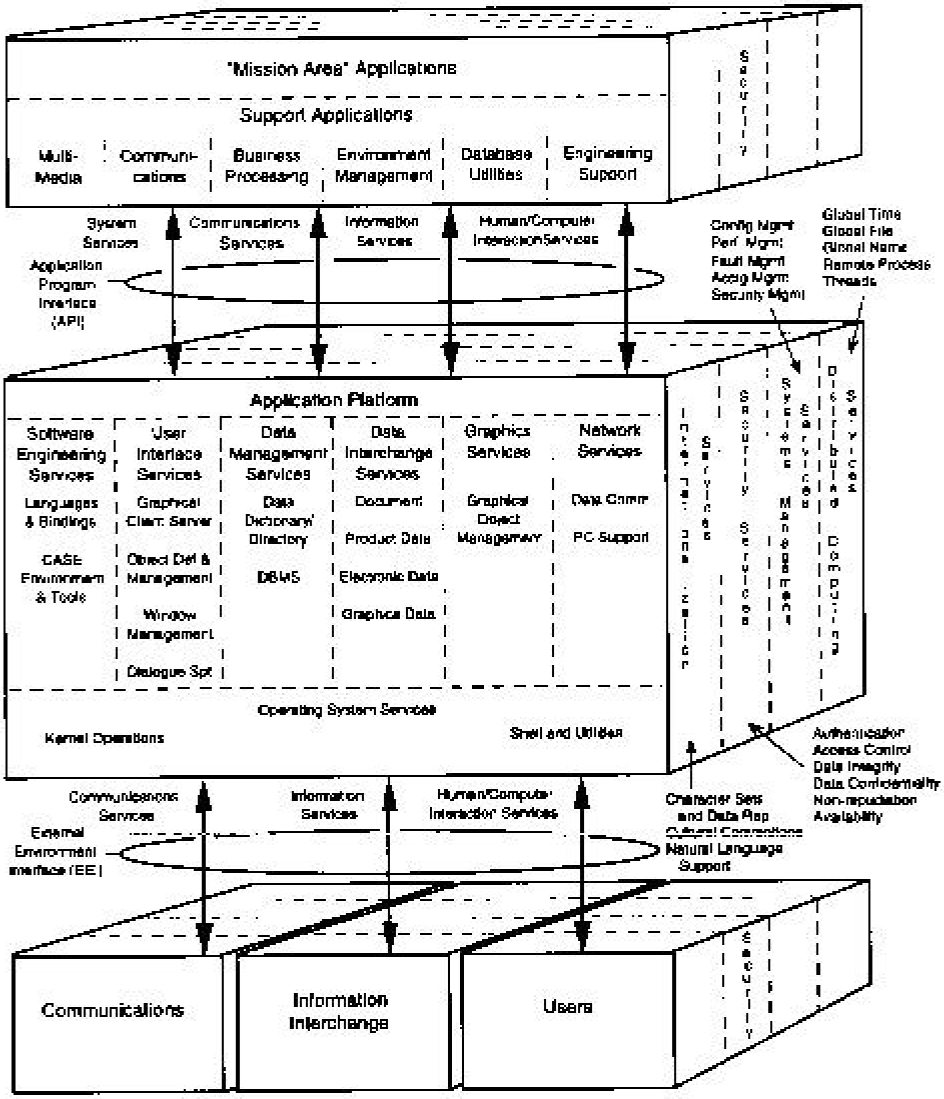


FIGURE 2-1 TAFIM TRM, VERSION 2.0

2.2 MANDATES

The ATA mandates the *COE concept* and the use of the Global Command and Control System (GCCS) COE APIs to speed software development and reduce software maintenance costs. The COE concept is described as a software architecture, an approach for building interoperable systems, a common collection of reusable software components, a software infrastructure, and a set of guidelines and standards. A detailed description of the of the COE concept is contained in the *DII COE Integration and Runtime Specification (I&RTS), Version 2.0, October 1995*. Since DII COE APIs are not yet available, software developers shall continue to use the GCCS COE APIs to access support application and application platform services. These

APIs are listed in the *GCCS COE 2.0 Baseline Document.* If a required service is not available in the COE APIs, software developed shall adhere to the individual processing standards in this section and the applicable domain appendix.

2.2.1 Application Software Entity

The Application Software Entity includes both mission area applications and support applications. Mission area applications implement specific user's requirements and needs (e.g. personnel, materiel management). This application software may be commercial off-the-shelf (COTS), government off-the-shelf (GOTS), custom-developed software, or a combination of these.

Support applications are common applications (e.g., E-mail and word processing) that can be standardized across individual or multiple mission areas and are the first layer of the COE. The services they provide can be used to develop mission-area-specific applications or can be made available to the user. The TAFIM TRM defines six support application categories: Multimedia; Communications; Business Processing; Environment Management; Database Utilities; and Engineering Support. The definitions of these categories are found in the TAFIM, Volume 2, Section 2.4.2.

The Application Software Entity includes all Army application software. All domains shall distinguish between their common support applications and mission area applications. Mission area applications shall use the GCCS COE support applications to the maximum extent possible. If a new support application must be developed, it shall use all applicable GCCS COE lower level application platform service APIs. In the absence of a standard interface to application platform services, developers will utilize the mandated individual standards contained in this section.

2.2.2 Application Platform Entity

The Application Platform Entity is the second layer of the COE, and includes the common, standard application platform services upon which the required functionality is built. The Application Platform Entity is used by the COE support applications and unique mission area applications software. The Application Platform Entity is composed of service areas and cross-area services. The definitions of these service areas are found in the TAFIM, Volume 2, Section 2.4.3. and 2.4.4 respectively. The corresponding mandates are provided in the following subsections.

2.2.2.1 Service Areas

The TAFIM TRM defines seven service areas within the Application Platform Entity: software engineering, user interfaces, data management, data interchange, graphics, network, and operating system services.

2.2.2.1.1 Software Engineering Services

The software engineering services provide system developers the tools appropriate to the development and maintenance of applications. These include programming languages, language bindings and object code linking, and Computer Aided Software Engineering (CASE) environments and tools. The following subsections specify applicable standards that such software engineering tools shall implement.

2.2.2.1.1.1 Programming Languages

Language services provide the basic syntax and semantic definition for use by developers to describe the desired software function.

Ada is mandated in DOD Directive 3405.1 for use in all DOD custom developed software. This mandate does not include software that is developed and maintained commercially. Software development shall be based on Ada 95. Ada 95 is backward-compatible with the Ada 83 language specification.

The *Assistant Secretary of Defense Memorandum, Subject: Delegations of Authority and Clarifying Guidance on Waivers from the Use of the Ada Programming Language* requires the DOD Services to implement a waiver process. Developers requesting an Ada waiver shall do so IAW HQDA LTR 25-92-1, *"Implementation of the Ada Programming Language,"* and extended by HQDA LTR 25-94-1 and HQDA LTR 25-95-1.

- ISO/IEC 8652:1995 (Ada 95), Ada Reference Manual, Language and Standard Libraries.

2.2.2.1.1.2 Language Bindings and Object Linking

Language bindings and object code linking provide the ability for software to access services and software through APIs that have been defined independently of the computer language. Ada bindings shall be used to provide the interface to COTS or GOTS software that is developed in other languages. The following standard is mandated.

- IEEE 1003.5:1992, POSIX: Ada Language Interfaces Part 1: Binding for System API

2.2.2.1.1.3 CASE Environments and Tools

CASE tools and environments include tools for requirements specification, design, analysis, creating, and testing code. The ATA does not mandate specific tools. Section 4 mandates standards that data modeling Computer Automated Software Engineering (CASE) tools will follow.

2.2.2.1.2 User Interface Services

These services *implement* the Human Computer Interface (HCI) style and control how users interact with the system. The ATA mandates X Window System and Open Software Foundation (OSF) Motif. The following standards apply:

- FIPS Pub 158-1, X Window System, Version 11, Release 5.
- OSF, 1992, Motif Application Environment Specification, Release 1.2
- OSF/Motif Inter Client Communications Convention Manual (ICCCM).

Refer to Section 5 for HCI style guidance and standards.

2.2.2.1.3 Data Management Services

Central to most systems is the sharing of data between applications. The data management services provide for the independent management of data shared by multiple applications. These services include data dictionary/directory services and database management systems (DBMS) services.

These services support the definition, storage, and retrieval of data elements from monolithic and distributed, relational DBMSs. These services also support platform-independent file management (e.g., the creation, access, and destruction of files and directories). The following standards are mandated for any system required to use a Relational Database Management System:

- FIPS Pub 127-2, Database Language - SQL.
- ISO 12227:1994, SQL Ada Module Description Language.

2.2.2.1.4 Data Interchange Services

The data interchange services provide specialized support for the exchange of data and information between applications and to and from the external environment. These services include document, graphics data, imagery data, product data, and electronic data interchange services. The standards below are mandated.

2.2.2.1.4.1 Document Interchange

These services provide the specifications for encoding data and the logical and visual structure of electronic documents.

- FIPS Pub 152, Standard Generalized Markup Language (SGML)-Interchange format for conveying the logical structure of office documents.
- IETF RFC 822 Version 3.0 Hyper Text Mark-up Language (HTML), - Interchange format used by the World Wide Web (WWW) for hypertext format and embedded navigational links.

2.2.2.1.4.2 Graphics Data Interchange

These services are supported by device-independent descriptions of picture element raster and vector graphics.

- MIL-STD 2411, Raster Product Format (RPF) - Defense Mapping Agency (DMA) format for raster-based products, such as Compressed ARC Digitized Raster Graphics (CADRG) and Controlled Image Base (CIB).

- MIL-STD 2407, Vector Product Format (VPF) - DMA format for vector-based products, such as Vector Map (Vmap), Digital Nautical Chart (DNC), Vector Interim Terrain Data (VITD), and World Vector Shoreline (WVS).
- MIL-D 89020, Digital Terrain Elevation Data (DTED) - DMA format used by DTED Levels 1 and 2.
- FIPS Pub 128, Computer Graphics Metafile (CGM) - Interchange format for vector graphics data.

2.2.2.1.4.3 Imagery Data Interchange

These services support still and motion picture services.

- ISO 11172, Motion Pictures Expert Group (MPEG) - Interchange format used for full-motion video and associated audio data.
- MIL-HDBK 1300A, National Imagery Transmission Format Standard (NITFS) - Interchange format for digital battlefield imagery and imagery-related products. NITFS provides a package containing information about the imagery, the image itself, and optional overlay graphics. Developed primarily for overhead photo imagery. NITFS is a suite of standards that includes: MIL-STD-2500A (file format); MIL STD-2301 (CGM for NITFS); and four separate compression algorithms (MIL-STD-188-196, MIL-STD-188-197A, MIL-STD-188-198A, and MIL-STD-188-199). Note that the Tactical Communications Protocol 2 (TACO2) identified within NITFS is not adopted by the ATA.
- ISO 10918-1, Joint Picture Expert Group (JPEG) - Interchange graphics format for photographs.

2.2.2.1.4.4 Product Data Interchange

These services include technical drawing specifications, documentation, and other data required for product design and manufacturing.

- MIL-PRF-28000A, Initial Graphics Exchange Specification (IGES) - Interchange format for computer-aided design (CAD) data, such as technical illustrations and engineering drawings.

2.2.2.1.4.5 Electronic Data Interchange

These services are used to create an electronic environment (paperless) for the exchange of data.

- FIPS Pub 161-1, Electronic Data Interchange (EDI) - Interchange format for documents that are highly structured (e.g., consisting of a sequence of numeric or alphanumeric fields rather than free-form text).

Refer to Section 4.2.4 for additional requirements on message standards.

2.2.2.1.5 Graphic Services

These services support the creation and manipulation of graphical images. These services include device-independent, multidimensional graphic object definition, and the management of hierarchical database structures containing graphics data. The standards that apply are:

- FIPS Pub 120-1 (change notice 1), Graphical Kernel System (GKS) - for 2-D graphics.
- FIPS Pub 153, Programmers Hierarchical Interactive Graphics Systems (PHIGS) - for 3-D graphics.

2.2.2.1.6 Network Services

These services support the distributed applications that require data access and applications interoperability in networked environments. The standards that apply are provided in Section 3.

2.2.2.1.7 Operating System Services

These core services are necessary to operate and administer a computer platform and to support the operation of application software. These services include kernel operations, shell and utilities. These services shall be accessed by applications through applicable standard Portable Operating System Interface (POSIX) APIs. Not all operating system services are required to be implemented, but those that are used shall comply with the standards. The following standards apply.

- IEEE 1003.1, POSIX: System API (with FIPS Pub 151-2 profile), POSIX: Portable Operating System Interface for Computer Environments
- IEEE 1003.2, POSIX: Shell and Utilities (with FIPS Pub 189-1 profile)
- IEEE 1003.2d, POSIX: Shell and Utilities - Batch Environment
- IEEE 1003.1c, POSIX: System API - Threads and Extensions
- IEEE 1003.1i, POSIX: System API - Real-time Extensions
- IEEE 1003.5:1992, POSIX: Ada Language Interfaces Part 1: Binding for System API

2.2.2.2 Application Platform Cross-Area Services

The TAFIM TRM defines four application platform cross-area services: internationalization, security, system management, and distributed computing services.

2.2.2.2.1 Internationalization Services

The internationalization services provides a set of services and interfaces that allow a user to define, select, and change between different culturally related application environments supported by the particular implementation. These services include character sets, data representation, cultural convention, and native language support.

In order to interchange text information between systems, it is fundamental that systems agree on the character representation of textual data. The following character set coding standards are mandated for the interchange of 8-bit and 16-bit textual information respectively:

- ISO/IEC 8859-1:1987, Information Processing - 8-Bit Single-Byte Coded Character Sets - Part 1: Latin Alphabet No. 1.
- ISO/IEC 10646-1:1993, Information Technology - Universal Multiple-Octet Coded Character Set (UCS) - Part 1: Architecture and Basic Multilingual Plane.

2.2.2.2.2 Security Services

These services assist in protecting information and computer platform resources. In order to fully meet security requirements, these services must often be combined with security procedures which are beyond the scope of the ATA. Security services include security policy, accountability, and assurance. Refer to Section 6 for security service standards.

2.2.2.2.3 System Management Services

These services provide capabilities to manage an operating platform and its resources and users. System management services include configuration management, fault management, and performance management. The standards that apply are provided in Section 3.2.1.4 .

2.2.2.2.4 Distributed Computing Services

These services allow various tasks, operations, and information transfers to occur on multiple, physically- or logically-dispersed, computer platforms. These services include global time, data, file and name services, thread services, and remote process services. The OSF Distributed Computing Environment (DCE) Version 1.1 standard is mandated. The standards that apply are:

- X/Open C309 - DCE Remote Procedure Call.
- X/Open C310 - DCE Time Services.
- X/Open C312 - DCE Directory Services.
- X/Open C403, DCE: X/Open Federated Naming (XFN) Specification.

2.3 EMERGING STANDARDS

2.3.1 DII COE

The Army is committed to the COE concept and will mandate the DII COE and associated APIs as they evolve. The GCCS COE will be phased out during calendar year 1996 and replaced with the DII COE. GCCS COE version 2.1 is the current version of the GCCS COE undergoing user evaluation. The DISA DII COE System Engineer plans to release GCCS COE version 2.2 by third quarter fiscal year 1996.

The DII COE will not support the original nineteen GCCS COE functional areas, however DISA has stated that the requirements for the GCCS COE functional areas will be preserved in the new DII COE taxonomy. The objective scope of the DII COE goes beyond GCCS and is intended to support all software systems developed in DOD. Initial releases of the DII COE will focus on GCCS and the Global Combat Support System (GCSS).

The DII COE will be organized into two major areas, Infrastructure Services and Common Support Applications:

- Infrastructure Services - These are the lower level functions provided for general workstation operation and management and generic application support. Infrastructure Services will be subdivided into five functional areas: Management Services (previously System, Security, and Network Administration), Presentation Services (previously Executive Manager and Multimedia Services), Data Access Services (previously Database Management Services, Data Administration, and File Management Services), Communications (previously Communications Services and Network Services) and Distributed Computing Services.
- Common Support Applications - The remainder of the GCCS COE areas (such as Correlation, Mapping Cartographic, Geospatial and Imaging (MCG&I), Message Processing, etc.) fall into this area.

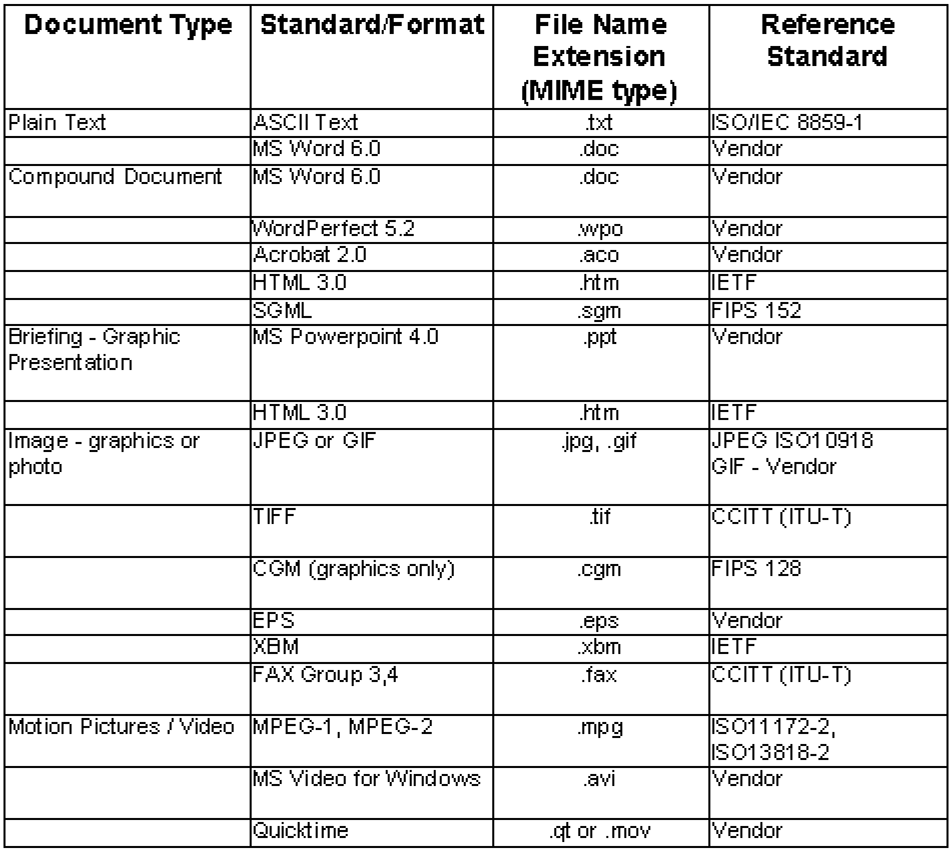
The DISA DII COE System Engineer has indicated that mission application developers should be targeting migration of applications to the DII COE instead of the GCCS COE. The first release of the DII COE will be made available to mission application developers in incremental versions during 1996. DII COE version 1.0 will be available to developers in early 1996. This release will contain the DII COE Developers Kit, the COE Kernel, and a limited set of infrastructure services. The Developers Kit will contain the initial set of DII COE APIs and their associated documentation, the DII COE Integration and Runtime Specification (I&RTS), the DII HCI Style Guide, and the DII COE Common Desktop Environment (CDE) Developers Guide. DII Version 2.0 is scheduled to be available to developers by the spring of 1996 and will contain the remainder of the Infrastructure Services and a limited set of Common Support Applications. The DII COE System Engineer has stated that these incremental versions will be additive and that the APIs to any service provided in an earlier version of the DII COE will remain essentially unchanged through later versions.

2.3.2 Service Area Standards

Within Data Interchange Services, wavelet image compression techniques are being reviewed for inclusion in the NITFS imaging standard. The ISO 13818, Motion Picture Experts Group (MPEG-2) is an emerging standard interchange format used for full motion video and associated audio data for data rates of 1.5 Mbps - 6.0 Mbps.

E-mail and FTP file transfer mechanisms are independent of the actual data file transported. The format of those files, however, is application-specific. To ensure the receiver of files can use the data, a common format must be specified and used by the sender. Guidelines for file formats used in the electronic exchange of documents via Email or file transfer are contained in Table 2-1. These file formats are NOT endorsements or mandates for specific vendor products. Many applications besides the original vendor's can read and write these formats. They are intended to represent the most capable, richest functional formats that are widely available and supported. Formats are listed in order of preference.

TABLE 2-1 ELECTRONIC DOCUMENT EXCHANGE FORMATS



Document Type	Standard/Format	File Name Extension (MIME type)	Reference Standard
Plain Text	ASCII Text	.txt	ISO/IEC 8859-1
	MS Word 6.0	.doc	Vendor
Compound Document	MS Word 6.0	.doc	Vendor
	WordPerfect 5.2	.wpo	Vendor
	Acrobat 2.0	.aco	Vendor
	HTML 3.0	.htm	IETF
	SGML	.sgm	FIPS 152
Briefing - Graphic Presentation	MS Powerpoint 4.0	.ppt	Vendor
	HTML 3.0	.htm	IETF
Image - graphics or photo	JPEG or GIF	.jpg, .gif	JPEG ISO10918 GIF - Vendor
	TIFF	.tif	CCITT (ITU-T)
	CGM (graphics only)	.cgm	FIPS 128
	EPS	.eps	Vendor
	XBM	.xbm	IETF
	FAX Group 3,4	.fax	CCITT (ITU-T)
Motion Pictures / Video	MPEG-1, MPEG-2	.mpg	ISO11172-2, ISO13818-2
	MS Video for Windows	.avi	Vendor
	Quicktime	.qt or .mov	Vendor

Note: Compound documents contain embedded graphics, tables and formatted text. Note that not all special fonts, formatting, or features supported in the native file format may convert accurately.

Within Operating System Services, it is expected that the draft IEEE P1003.x POSIX standards will be adopted once they become final. In addition, the X/Open Single UNIX Specification (SUS) (previously referred to as Specification 1170) is an emerging standard. It is also expected that POSIX, 1003.5b will be approved in 1996 which will deal with real-time interfaces and Ada 95 improvements as well as provide a "wide" character set suitable for dealing with Asian languages.

Within Distributed Computing Services, the emerging standards include the Common Object Request Broker Architecture (CORBA) 2.0 and DCE Authentication and Security Specification (P315).

Within Data Management Services, the emerging standards include the ISO/IEC 9075-3, 1995 Call Level Interface, and draft DIS 9075-4, Database Language SQL, Part 4: Persistent Stored Modules (SQL/PSM).

This page was intentionally left blank.

SECTION 3

INFORMATION TRANSPORT STANDARDS

3.1 INTRODUCTION

3.1.1 Purpose

Information transport standards and profiles are described in this section. These standards provide seamless communications and information transport interoperability for Army systems.

3.1.2 Scope

The standards described in this section apply at the external interfaces between computer systems (i.e., hosts), routers, and communications networks. These standards do not apply at the interfaces between hosts and peripherals (e.g., storage devices, sensors, and weapons control). Where operational or system requirements dictate the need for tactical data links, the data link standards in Section 4.2.4.4 shall apply.

3.1.3 Background

The standards herein are drawn from widely accepted, commercial standards. In particular, the ATA makes use of the same open-systems architecture used for the Internet and the Defense Information Systems Network (DISN). These networks provide for communications interoperability between systems that may be on different communications networks.

3.1.3.1 Communications Framework

System components are categorized here as hosts, networks, and routers. Hosts are computers that generally execute application programs on behalf of users and share information with other hosts via networks. Networks may be relatively simple (e.g., point-to-point links) or have complex internal structures (e.g., network of packet switches). Routers interconnect two or more networks and forward packets across network boundaries. Routers are distinct from hosts in that they are normally not the destination of data traffic.

Host standards are specified in Section 3.2.1. Router standards are specified in Section 3.2.2. Within the OSI reference model, the standards in these sections map to the internetwork layer and above. These standards support logical end-to-end interface connections. Hosts and routers connect to networks using the corresponding network interface protocols. The network protocols correspond to the physical, data link, and intranet layers that are defined by the Open Systems Interconnection (OSI) reference model. Network standards are specified in Section 3.2.3.

3.1.3.2 Protocol Standards

A number of the standards mandated in this section are published by the Internet Architecture Board (IAB). The IAB is responsible for the Internet Protocol (IP) suite, and documents these protocols using Request for Comments (RFCs) and Standards (STDs). STDs are a subseries of notes within the RFC series that are formal Internet "Standards." When a protocol is defined by both an RFC and a STD, the ATA uses the STD nomenclature.

The ATA mandates only a small subset of protocols within the entire IP suite. Other protocols within the IP suite can be used if they provide services that are not offered by any of the mandated protocols.

3.1.3.3 Protocol Profiles

Protocol standards generally have multiple options and parameters that can assume a range of values. Some of these options and parameters have local significance, and can be selected to optimize performance or provide unique services for a specific application. Other options and parameters have global significance, and must be consistent across multiple applications to support seamless communications.

To foster interoperability, a profile is established for each protocol standard that has options and parameters with global significance. The profile imposes particular values for these options and parameters. The profiles are listed in Section 3.2 next to their corresponding standards.

Many of the profiles are documented in the MIL-STD-2045-1xxxx series. These profiles are developed by the DOD Information Transfer Standards Management Panel (IXMP). At this time, MIL-STD-2045-1xxxx profiles do not exist for every standard specified in this section. However, the intent is to develop profiles as they are needed.

3.2 MANDATES

3.2.1 Host Standards

All hosts shall adhere to STD-3. This is an umbrella standard that references other documents and corrects errors in some of the referenced documents. STD-3 also adds additional discussion and guidance for an implementor.

3.2.1.1 Internetwork Layer Standards

STD-5 shall be used at the internetwork layer. STD-5 defines the IP protocol, which is a basic connectionless datagram service. All protocols within the IP suite use the IP datagram as the basic data transport mechanism. IP was designed to interconnect heterogeneous networks and operates over a wide variety of networks.

Within STD-5, two other protocols are considered integral parts of IP: the Internet Control Message Protocol (ICMP) and the Internet Group Management Protocol (IGMP). ICMP is used to provide error reporting, flow control, and gateway redirection. IGMP provides multicast extensions for hosts to report their group membership to multicast routers.

The profile for STD-5 shall be in accordance with MIL-STD-2045-14502-1A.

3.2.1.2 Transport Layer Standards

Either STD-6 or STD-7 shall be used at the transport layer. These two protocols provide fundamentally different services. STD-6 defines the User Datagram Protocol (UDP), which provides a connectionless, datagram service to applications not requiring reliable, sequenced communications. STD-7 defines the Transmission Control Protocol (TCP), which provides a reliable, connection-oriented transport service.

The profile for STD-6 and STD-7 shall be in accordance with MIL-STD-2045-14502-1A.

3.2.1.3 Application and Support Standards

- *File transfer* - Basic file transfer shall be accomplished using the File Transfer Protocol (FTP) protocol. FTP provides a reliable, file transfer service for text or binary files. While designed to be used by other programs, it includes a direct interactive user interface to enable access to remote file servers. FTP, which uses TCP as a transport service, is specified in STD-9. The profile shall be in accordance with MIL-STD-2045-17504.

- Remote terminal - Basic remote terminal services shall be accomplished using TELNET. TELNET provides a virtual terminal capability that allows a user to "log on" to a remote system as though the user's terminal was directly connected to the remote system. TELNET, which uses TCP as a transport service, is specified in STD-8. The profile shall be in accordance with MIL-STD-2045-17506.

- Electronic mail - The standard for electronic mail is Defense Message System (DMS)-compliant X.400. This provides a full-featured, electronic mail service, as specified in Allied Communication Publication (ACP) 123 and AMHS 1 (U.S. Supplement to ACP 123). The profile for common messaging is specified in MIL-STD-2045-17501. The profile for military messaging services is specified in MIL-STD-2045-17502. The profile for the Message Security Protocol (MSP) is specified in MIL-STD-2045-18500. Note that X.400 is not an Internet standard, and must operate over TCP through the use of STD-35 and MIL-STD-2045-14503.

- Directory services - International Telecommunications Union (ITU) X.500 provides directory services that may be used by users or host applications to locate other users and resources on the network. X.500 also provides security services used by DMS-compliant X.400 implementations. Note that X.500 is not an Internet standard, and must operate over TCP through the use of STD-35 and MIL-STD-2045-14503.

- *Booting without disks* - The BootStrap Protocol (BOOTP) provides a mechanism for a diskless system to initialize itself from a server. BOOTP, which uses UDP as a transport service, is specified in RFC-951, with additional clarifications provided in RFC-1542.

- *Dynamic configuration* - The Dynamic Host Configuration Protocol (DHCP) is used to dynamically assign an IP address and provide other information necessary to configure a host to operate on a network. DHCP consists of two parts: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for automatically allocating IP addresses to hosts. DHCP, which uses UDP as a transport service, is specified in RFC-1541.

- *Hypertext transfer* - The HyperText Transfer Protocol (HTTP) is used to support hypertext search and retrieval. HTTP, which uses TCP as a transport service, is defined in an Internet Draft. Uniform Resource Locators (URLs), which specify how objects are identified with HTTP, are defined inRFC-1738 and RFC-1808.

- *Translating names to addresses* - The Domain Name System (DNS) provides the service of translating between host names and IP addresses. DNS, which uses TCP as a transport service, is specified inSTD-13. The profile shall be in accordance with MIL-STD-2045-17505.

- *Connectionless application layer* - MIL-STD-2045-47001 provides a connectionless application layer for the transfer of Variable Message Format (VMF) messages. This standard identifies the intended destinations by name; privacy/security mechanisms required; data syntax constraints; and quality-of-service parameters. Furthermore, the standard provides synchronization of cooperating application processes; message handling; and message transfer via a connectionless operation. MIL-STD-2045-47001 uses UDP as a transport service.

3.2.1.4 Network Management Standards

Network management provides the capability to manage designated network(s). This includes the capability to control the network's topology; dynamically segment the network into multiple logical domains; maintain network routing tables; monitor the network load; and make routing adjustments to optimize throughput. Network management also provides the capability to review and publish network addresses of network objects; monitor the status of network objects; start, restart, reconfigure or terminate network objects; and detect loss of network objects in order to support automated fault recovery.

To support the net management service, hosts shall implement the SNMP set of management protocols. The set consists of STD-15 (Simple Network Management Protocol), STD-16 (Structure of Management Information), and STD-17 (Management Information Base). The profile for these STDs shall be in accordance with MIL-STD-2045-17507. SNMP uses UDP as a transport service.

3.2.1.5 Video Teleconferencing (VTC) Standards

ITU H.320 is mandated for video teleconferencing at data rates of 56 - 1920 kbps. ITU H.324 is mandated for video teleconferencing at data rates of 28.8 kbps and below. Both of these are umbrella standards that cite other ITU standards for video teleconferencing, such as audio and video compression and communications framing.

The *Industry Video Teleconferencing Profile*, as developed by the Corporation for Open Systems (COS), is mandated as the VTC profile. The purpose of the profile is to provide interoperability between VTC terminal equipment. This profile is based on the ITU H.32x series of recommendations for video teleconferencing. This industry profile was adopted by DOD as the official VTC standards document, per ASD (C3I) memorandum, dated 31 October 1994.

3.2.1.6 Global Position System (GPS) Standards

GPS User Equipment must employ Precise Position Service (PPS) user equipment incorporating both Selective Availability and Anti-Spoofing features to support combat operations. The GPS guidelines that are documented in ASD Memorandum *Development, Procurement, and Employment of DoD Global Position System User Equipment, 31 April 1992* must be followed. Emerging interface standards between hosts and GPS are identified in Section 3.3.1.

3.2.2 Router Standards

All routers shall adhere to STD-4. This is an umbrella standard that references other documents and corrects errors in some of the referenced documents. STD-4 also adds additional discussion and guidance for an implementor.

Some of the standards that were mandated for hosts in Section 3.2.1 also apply to routers. Specifically, the following standards apply to routers: IP (STD-5), UDP (STD-6), TCP (STD-7), TELNET (STD-8), DNS (STD-13), and SNMP (STD-15, STD-16, and STD-17).

Routers exchange connectivity information with other routers to determine network connectivity and adapt to changes. This enables routers to determine, on a dynamic basis, where to send IP packets.

- *Interior routing* - Routes within an Autonomous System (AS) are considered local routes that are administered and advertised locally by means of an interior gateway protocol. Routers shall use the Open Shortest Path First (OSPF) V2 protocol for interior gateway routing. OSPF V2, which uses IP directly, is specified inRFC-1583. A profile for this standard is not currently available.

- *Exterior routing* - Exterior gateway protocols are used to specify routes between ASs. Routers shall use the Border Gateway Protocol (BGP) V4 for exterior gateway routing. BGP V4, which uses TCP as a transport service, is specified in RFC-1654. The profile shall be in accordance with MIL-STD-2045-13502.

3.2.3 Network Standards

This section identifies the network interface standards that have been adopted by the ATA. These standards support a range of performance needs. The selection of specific network standards for a given application should be based on system-related requirements, such as cost and speed-of-service.

These standards operate at the physical and link layers, and in some instances, at the intranet sublayer of the network layer. These standards are not generally defined by RFCs. However, RFCs are used to define how these networks interface with IP (e.g., address resolution). The protocol standards and corresponding profiles are given in the following subsections.

3.2.3.1 Serial Lines

Serial lines provide full-duplex, point-to-point communications links. The physical layer shall be in accordance with RS-232, RS-422/423/449, RS-530, or MIL-STD-188-114A. Four-wire, conditioned diphase, as specified in MIL-STD-188-200, may be used where appropriate. The data link layer shall be as follows:

- *Asynchronous* - For asynchronous lines, the data link protocol shall be the Point-to-Point Protocol (PPP), which is specified in STD-51. The profile is specified in MIL-STD-2045-13500-2.

- *Synchronous* - For synchronous lines, the data link protocol shall be either PPP or the Link Access Protocol Balanced (LAPB) protocol, as specified in ITU X.25, Section 2. The profile for LAPB is specified in MIL-STD-2045-14502-2.

3.2.3.2 Ethernet

Ethernet is the most common network technology available. Data is transmitted at 10 Mbps over a cable, which is shared by multiple hosts. The hosts use a carrier sense multiple access with collision detection (CSMA/CD) scheme to control access to the cable. At the physical layer, Ethernet shall be implemented with any of four different types of cable. The implementations (and cable types) shall be as defined by the IEEE as: 10Base-5 (thick coaxial); 10Base-2 (thin coaxial); 10Base-T (unshielded twisted pair); and 10Base-F (fiber-optic cable).

Ethernet's physical layer and CSMA/CD access scheme are specified in IEEE 802.3. The interface between Ethernet and IP shall be in accordance with STD-41 and STD-43. The profile for Ethernet shall be in accordance with MIL-STD-2045-14502-4/5.

For higher-speed requirements, 100-Mbps Ethernet technology shall be implemented in accordance with the Fast EtherNet standard, IEEE 802.3u. This standard supports auto-negotiation of the media speed, making it possible for dual-speed Ethernet interfaces to run at either 10 or 100 Mbps automatically.

3.2.3.3 Fiber Distributed Data Interface (FDDI)

FDDI is a mature high-speed network standard. Data is transmitted at 100 Mbps over either multimode or singlemode fiber-optic cable. FDDI is defined by a series of International Organization for Standardization (ISO) standards. These standards shall apply: 9314-1 (physical layer), 9314-2 (media access control), and 9314-3 (medium dependent). In addition, the Station Management (SMT) protocol defined in ANSI X3.229 shall be used.

The Logical Link Control (LLC) layer for FDDI shall be as specified in IEEE 802.2. The interface between FDDI and IP shall be in accordance with STD-36.

3.2.3.4 Asynchronous Transfer Mode (ATM)

ATM is a high-speed switching technology that takes advantage of low bit-error rate transmission facilities to accommodate intelligent multiplexing of voice, data, video, imagery, and composite inputs over high-speed trunks. The network access protocols to ATM switches are defined in the ATM Forum's User-Network Interface Specification, Version 3.1. These network access protocols can operate over fiber-optic and twisted pair cables, with data rates of 1.5, 45, 100, and 155 Mbps. In addition, a 25.6 Mbps interface is supported in accordance with *25.6 Mb/s over Twisted Pair Cable Physical Interface*.

The protocol layers consist of an ATM Adaptation Layer (AAL), the ATM layer, and a physical layer. The role of AAL is to divide the variable-length data units into 48-octet units to pass to the ATM layer. There are currently four defined AAL protocols to support different service classes. The ATA mandated two of these AAL protocols. AAL1 shall be used to support constant bit rate service, which is sensitive to cell delay, but not cell loss. AAL5 shall be used to support variable bit rate service. IP packets shall be transported over AAL5, in accordance with RFC-1577.

3.2.3.5 X.25

X.25 is an international standard that has been widely adopted for packet-switched networks. X.25 defines the interface between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE). The DTE generally refers to the router or host equipment side of the interface, and the DCE refers to the communications network side.

The standards that apply to DTEs are different from (but fully compatible with) the standards that apply to DCEs. For DCEs, ITU X.25 shall be used at the data link and packet (i.e., intranet) layers. For DTEs, ISO 7776 shall be used at the data link layer and ISO 8208 shall be used at the packet layer.

At the physical layer, the X.25 interface shall be in accordance with RS-232, RS-422/423/449, RS-530, or MIL-STD-188-114A. Four-wire, conditioned diphase, as specified in MIL-STD-188-200, may be used where appropriate.

The method of interworking IP with X.25 interfaces shall be as specified in RFC-1356. For the X.25 interface to the Army Data Distribution System (ADDS), the profile shall be in accordance with ACCS-A3-407-008D. For all other X.25 interfaces, the profile shall be in accordance with MIL-STD-2045-14502-3.

3.2.3.6 Integrated Services Digital Network (ISDN)

ISDN is an international standard used to support integrated voice and data over standard twisted-pair wire. ISDN defines a Basic Rate Interface (BRI) and Primary Rate Interface (PRI) to provide digital access to ISDN networks. These interfaces support both circuit-switched and packet-switched services.

The BRI and PRI physical layers are specified by I.430 and I.431, respectively. The profiles for BRI and PRI are National ISDN 1 and 2, respectively. The BRI physical layer uses two wires to provide two B channels (64 kbps) for information transport and one D channel (16 kbps) for signaling. The PRI physical layer uses four wires to provide 23 B channels (64 kbps) for information transport and one D channel (64 kbps) for signaling. The B channels can provide clear channel services or packet based, point-to-point services.

For B channels configured for packet-switched services, the data link and network layers shall be the same as specified in X.25. IP packets shall be encapsulated and transmitted over ISDN as specified in RFC-1356. For B channels configured for clear channel services, IP packets shall be encapsulated and transmitted using PPP over ISDN as specified in RFC-1618.

For D channels, the data link layer is specified in Q.921 and the network layer is specified in Q.931.

3.2.3.7 MIL-STD-188-220A

Combat Net Radios (CNRs) are a family of radios that provide voice and data communications for mobile users. These radios provide a half-duplex, broadcast transmission media with potentially high bit error rates. With the exception of High Frequency (HF) networks, MIL-STD-188-220A shall be used as the standard communications net access protocol for CNR networks and other Force XXI Battle Command Brigade and Below (FBCB2) systems requiring interoperability over CNR. The method by which IP packets are encapsulated and transmitted is specified in MIL-STD-188-220A. The profile shall be in accordance with MIL-STD-2045-14502-6A.

3.2.4 Summary of Packet Standards

For reference purposes, Figure 3-1 shows a summary of the information transport standards used for packet-switching that are mandated within the ATA.

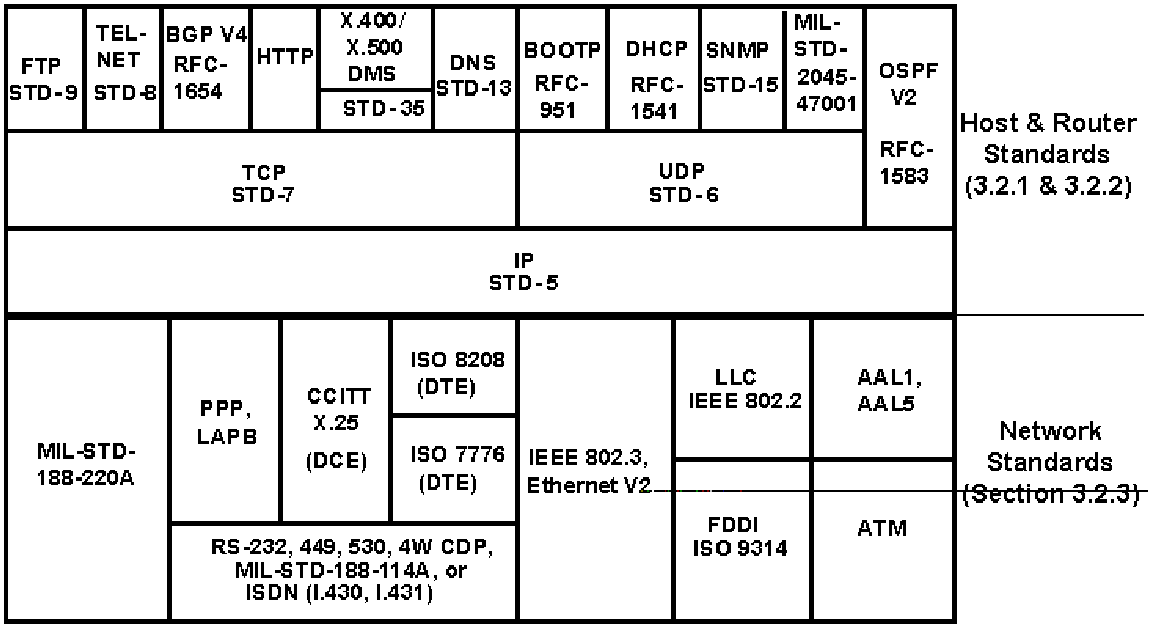


FIGURE 3-1. SUMMARY OF THE PACKET-SWITCHED TRANSPORT STANDARDS

3.3 EMERGING STANDARDS

Commercial communications standards and products will evolve over time. The ATA must evolve, as well, to benefit from these standards and products. The purpose of this section is to provide notice of those standards that are not yet a part of the ATA, but are expected to be adopted in the near future.

3.3.1 Emerging Host Standards

- *Common Management Information Protocol (CMIP)* - CMIP is evolving and is generally accepted for switched telecommunications services. While CMIP is not mandated in the ATA, it is recognized as a protocol in current use within designated Army systems. It is expected that CMIP will evolve/coexist with SNMP to share parameters and agents in common, with added capabilities and a new manager-to-manager relationship.

- *IP multicast routing protocols* - It is expected that multidestination addressing will evolve from Selective Directed Broadcast Mode (SDBM), as defined in RFC-1770, to IP multicast. IP multicast uses Class D group addresses. Both host-to-router and router-to-router multicast protocols are required to share group information. The host-to-router protocol is IGMP, which is specified in STD-5. There are several router-to-router protocols, but these are not currently mature Internet standards. One of the following standards may be adopted in the near future: Distance Vector Multicast Routing Protocol (RFC-1075), Multicast OSPF (RFC-1584), or Protocol Independent Multicast (Internet Draft).

- *IP Next Generation/Version 6 (IPV6)* - IPV6 is being designed to provide better internetworking capabilities than are currently available within IP (Version 4). IPV6 will include support for: (1) expanded addressing and routing capabilities, (2) a simplified header format, (3) extension headers and options, (4) authentication and privacy, (5) autoconfiguration, (6) simple and flexible transition to IPV6, and (7) increased quality of service capabilities.

- *Mobile Host Protocol* - The primary aim of this protocol is to provide information reachability for the mobile host. The intent is that a mobile host should not have to perform any special actions because of host migration. A mobile IP protocol is currently available as an Internet draft, entitled IP Mobility Support.

- *VTC Standards* - There are two emerging VTC standards that support communications over different networks. ITU H.321 and ITU H.323 are draft recommendations that support VTC over ATM and Ethernet networks, respectively.

- *GPS Standards* - For the GPS standard, the following Interface Control Documents (ICDs) are under review: User Equipment ICD for the RS-232/RS-422 Interface of DoD Standard GPS User Equipment Radio Receivers (Draft) (ICD-GPS-153); GPS Receiver Application Module Interface, Parallel Dual Port Interface (Draft) (ICD-GPS-155); and Precise Time and Time Interval (PTTI) Interface, Rev A (ICD-GPS-060).

3.3.2 Emerging Network Standards

- *ATM-related standards* - Three ATM-related standards are identified as emerging. First, the ATM Forum is developing Private Network-Network Interface (PNNI) routing and signaling standards to support large, dynamic, multivendor ATM networks. PNNI routing will automatically disseminate network topology and resource information to switches in the network, enabling quality-of-service sensitive routing. Using this information, PNNI signaling will allow calls to traverse large, dynamic networks in a scaleable fashion. Second, Ethernet can be emulated over ATM networks using ATM Local Area Network Emulation (LANE), Version 1.0. This permits ATM networks to be deployed without disruption of end-system network protocols and applications. Third, the DOD is developing a standardized profile for ATM. The profile is a selection of base standards, options and parameters to facilitate interoperability. This profile is specified in the draft MIL-STD-188-176.

- *Wireless network standards* - The IEEE 802.11 Committee is developing standards for wireless services across three transmission media: spread-spectrum radio; narrowband radio; and infrared light. Wireless technology is useful in environments requiring mobility of the users or flexible network establishment and reconfiguration.

This page was intentionally left blank.

SECTION 4

INFORMATION MODELING AND DATA EXCHANGE STANDARDS

4.1 INTRODUCTION

4.1.1 Purpose

This section identifies the minimum information standards applicable to information modeling and exchange of information for all systems. Information standards pertain to activity or process models, data models, data definitions, and data exchange.

4.1.2 Scope

This section provides implementation direction affecting the definition, design, development, and testing of information models and data exchange among systems. It is applicable at all organization levels and environments (e.g., tactical, strategic, sustaining base, and interfaces to weapons systems). This chapter is divided into two sections: data standardization and data exchange. Data Standardization mandates apply to all systems or components of systems. Data Exchange mandates apply to all information components that must interact with any external system or device. For example, some systems are in completely enclosed environments (e.g., an on-board missile guidance system that must signal to the weapon's on-board steering control) and may not need to comply specifically with these sections. The materiel developer must determine if his particular system or component within the system requires ANY interaction with the external environment. Those systems or components that require an external interface must adhere to the Data Exchange Standards. If in doubt, plan for interoperability until the system requirements determine otherwise.

The relationship of the Information Standards to the TAFIM is illustrated in Figure 4-1. Process models identify functionality required of mission area applications and identify the information required in the data model. The data model identifies the logical information requirements and metadata, which will be developed into physical database schemata and standard data elements. Once implemented in operational systems, the data will be shared using generic data exchange standards.

4.1.3 Background

An information model is a representation at one or more levels of abstraction of a set of real-world processes, products, and interfaces. A process (or activity) model is a representation of a mission area application, composed of one or more related activities, and data (i.e., abstract data types) is the product of each activity. A data model defines entities and their data elements and illustrates the entities' interrelationships. An interface model ties disparate processes together for some combined functionality. This chapter focuses on the use of process and data models. Interface models are customized to fit a particular project, hence system developers should create and use interface models as necessary.

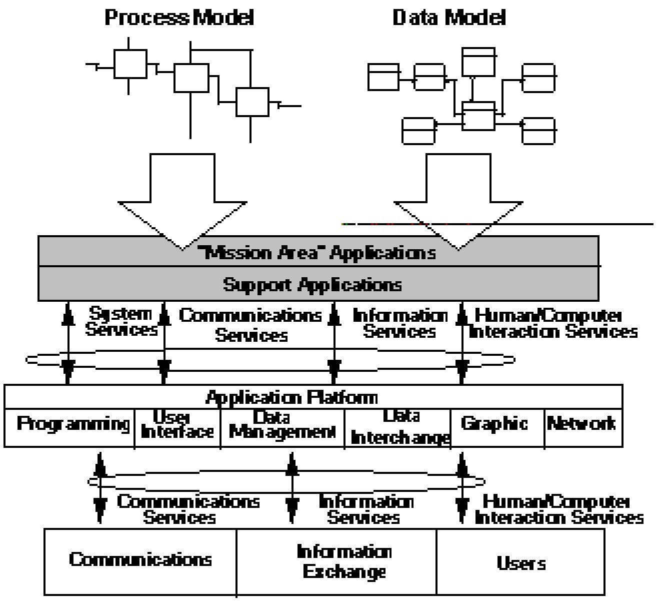


FIGURE 4-1. RELATIONSHIP OF TAFIM TO INFORMATION STANDARDS

To support the identification of information and information interchange requirements, the DOD has selected the **I**ntegrated Computer Aided Manufacturing **DEF**inition (IDEF) modeling methodology. DOD Directive 8320.1-M requires IDEF0 in accordance with FIPS Pub 183 and IDEF1X in accordance with FIPS Pub 184 as the standard for function method and extended data method, respectively. The IDEF Modeling methodology defines an unambiguous set of the following components:

- Symbols (i.e., syntax) associated with modeling concepts and ideas.
- Rules for composing these symbols into abstract constructs.
- Rules for mapping "meanings" (i.e., semantics) to these constructs.
- Definitions of the relationships between activities and entities.

Information Standards define a logical view of data (meaning and contextual use) within an architecture. The process model is a view of the activities, both automated and manual, that an organization must perform in order to achieve its mission. Modeling an organization's processes and data begins at the highest logical level, is decomposed into lower logical levels and is communicated in a format that the users, particularly the subject matter experts, can easily understand and use.

In order to provide a single authoritative source for data definitions and documentation standards, the DOD created the Defense Data Dictionary System. The DDDS, which is managed by the Defense Information Systems Agency (DISA), is a DOD-wide central database that includes standard data entities, data elements and, soon, data models. The DDDS is used to collect and integrate individual data models into a DOD enterprise data model and to document content and format for data elements. Recent studies show three necessary data characteristics must be known to define interoperable databases. First, the context view of data must be developed to understand how data elements interact with each other. Second, the terms data definitions must be unambiguous. Third, the foreign key identifiers must be defined in parent to child data relationships. These characteristics are contained within the combination of the DDDS, IDEF0 and IDEF1X models. Figure 4-2 provides an objective view of how the process and data modeling standards contained in this section will support the development of interoperable systems.

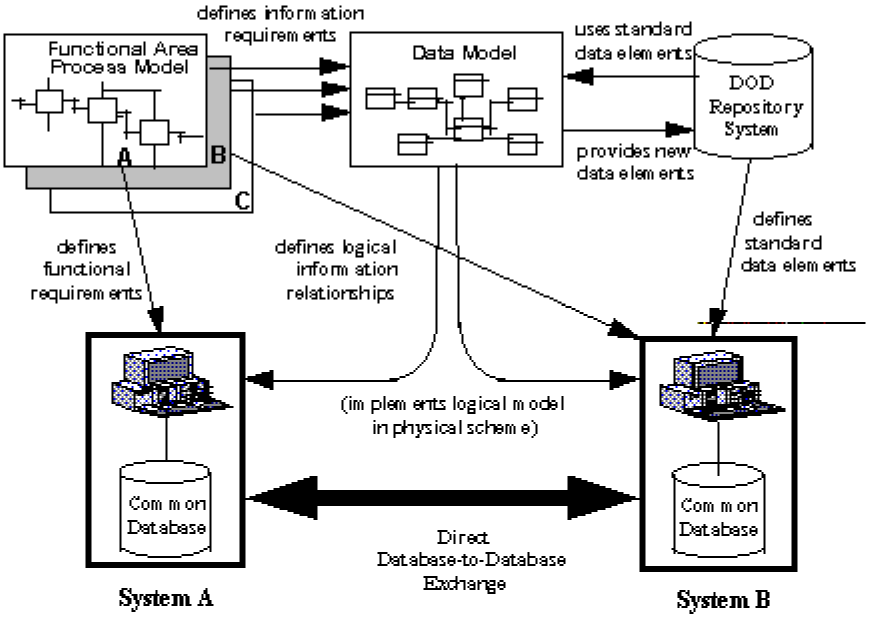

defines information requirements
Functional Area Process Model
A
B
C
Data Model
uses standard data elements
DOD Repository System
provides new data elements
defines standard data elements
defines functional requirements
defines logical information relationships
(implements logical model in physical scheme)
Common Database
Common Database
Direct Database-to-Database Exchange
System A
System B

FIGURE 4-2. OBJECTIVE INFORMATION EXCHANGE ARCHITECTURE

Today, battlefield information exchange is accomplished by sending messages. The definition and documentation of these messages are provided by various messaging standards, such as Variable Message Format (VMF), and the U.S. Message Text Format (USMTF). Each message standard provides a means to define message form and functions (i.e., transfer syntax), which includes the definition of the message fields that are contained in each message. The message fields, which are currently defined in the various message standards, are not mutually consistent across message types, nor are based on any process or data models, either within a message system or across message systems. Newer techniques can provide direct database-to-database exchange of data, without the user having to follow a rigid format. To use these newer techniques, the message fields must be converged with the data element set that is developed through the process and data modeling efforts defined in this section (4.2.1 and 4.2.2). This set is compliant with the Department of Defense data element standards established in accordance with the DOD 8320.1 series of directives.

4.2 MANDATES

4.2.1 Process Model

System acquisition and development begin with the identification of the need (Mission Need Statement) for a system to rectify a capability deficiency and the development of an Operational Requirements Document (ORD). Prior to beginning system development (Milestone II) and prior to major software upgrades to existing systems, the ORD shall be used to model information products and requirements using the IDEF0 methodology (FIPS Pub 183) to a level of detail sufficient to identify each entity in the data model that is involved in an activity. The activity model shall form the basis for data model development or refinement. The activity model will be validated against the requirements document and doctrine and then approved by the combat developer. The process model that is contained in the DOD Process Model Repository (currently managed by the Army Corps of Engineers) shall be used as a reference for extending activity models for specific programs.

The doctrinally based process models shall be used to describe the baseline functional and interface requirements. These models will normally be used in systems development in the system's User Functional Description (UFD). System developers can maintain traceability of requirements back to these process models. The process model will be enhanced and refined to accommodate the increased knowledge inherent in system development. An approved process model, by the materiel developer, can support criteria for Milestone II and III decisions.

As activity models are developed, security levels shall be considered. Most process models are unclassified even if the content of one or more activity characteristics (see ICOM below) is classified. However, if the developer determines that parts of the model must contain classified information, appropriate regulatory safeguards will be met. Different parts of the models can be labeled with different security labels. It must be possible to classify an entire model or to classify only certain activities and inputs, controls, outputs, and mechanisms (ICOM) within a model. Activities and ICOMs must have a provision for hierarchical (e.g., SECRET, TOP SECRET) and non-hierarchical (e.g., US ONLY, RELROK) security classification levels for the case where the model is unclassified, but the data is classified. It must be possible for a model to assume a range of security classification levels during its life cycle development as requirements are refined. It must be possible to classify a previously unclassified model when it is re-used within a different context.

4.2.2 Data Model

The basis for data modeling shall be the DOD Enterprise Data Model (EDM). The EDM is a corporate-wide data model that provides the standard meaning and use of specific data elements to the developers of all DOD systems. Adherence to the EDM will ensure DOD agencies are data interoperable among all systems. Tactical systems must incorporate applicable C2 Core Data Model (C2CDM) elements. The C2CDM is a part of the EDM. Both reside in the DDDS. It provides the tactical metadata and modeling elements for all DOD. New information requirements that are derived from activity models and approved through the DOD Data Standardization Program (DODD 8320 Series) will be used to extend the EDM and C2CDM as appropriate. Computer Automated Software Engineering (CASE) tools that support IDEF1X diagrams shall be used to extend the model with additional logical entities, attributes, and relationships. The IDEF1X syntax and diagramming conventions shall be in accordance with FIPS Pub 184. Data model development shall proceed in accordance with DOD 8320.1-M-X.

The data models shall be used in software requirements analyses and design activities as a logical basis for physical database design. Developers of new and existing systems shall maintain traceability between their physical database schema and the EDM and C2CDM, as applicable, allowing links from interface requirements to database population and update processes. A top level data model will be prepared for Milestone II decisions; a fully attributed data model will be assessed during the Preliminary Design Review and Critical Design Review.

As data models are developed, security levels and caveats shall be considered. Most data models are unclassified even if the content of one or more data elements is classified. However, if the developer determines that parts of the model must contain classified information, appropriate regulatory safeguards will be met.

4.2.3 Data Definitions

System developers shall use the DDDS as a primary source of data element standards. DOD Directive 8320.1-M provides the procedures for Data Administration. DOD 8320.1-M-1 provides data element standardization procedures. A classified version of the DDDS is being developed to support standardization of classified data elements and data models.

4.2.4 Data Exchange

4.2.4.1 Data Exchange Applicability

This section covers the exchange of information among mission area applications within the same system or among different systems. This is the scope of the term "data exchange." The exchange of information among applications shall be based on the logical data models developed as the result of identifying information requirements through activity or process models. The data model identifies the logical information requirements, which shall be developed into physical database schemata and standard data elements. The standard data elements shall be exchanged using the data management, data interchange and distributed computing services of application platforms (Refer to Section 2 for further guidance on these services). The intent is to exchange information directly between systems without the constraint of formatted messages.

For purposes of this document we must clarify subtle differences between "data exchange" and "data interchange." Data Exchange is the system or *application-independent* ability of data elements to be shared. Data Interchange, on the other hand, is system or *application-specific* sharing of objects such as documents, images, etc. Hence, this section discusses data exchange as the *generic* ability of a system or application to share data. Data Interchange standards, such as JPEG, form part of the DII COE and facilitate the sharing of data through the use of system or application *formats*. Key references include Section 2.2.2.1.3, for SQL standards in Data Management Services, and Section 2.2.2.1.4 for Data Interchange Services.

The message sets described below are mandated as an interim means of transferring information until mechanisms that use standard data elements are approved. *DISA is the proponent for information exchange using standard data.*

4.2.4.2 Variable Message Format (VMF) Messages

VMF messages shall be used for information transfer between systems requiring variable bit-oriented messages. VMF messages are specified in the Task Force XXI VMF Technical Interface Design Plan (TIDP). For systems requiring Joint VMF messaging, refer to Section 4.2.4.4.

4.2.4.3 US Message Text Format (USMTF) Messages

USMTF messages will be used when required for Joint interoperability if standard data exchange is not possible. USMTF messages are documented in MIL-STD-6040 (formerly JCS Publication 6-04). USMTF messages are character based and usually limited to the teletype character set.

4.2.4.4 Tactical Digital Information Link (TADIL-J Series) Messages

The TADIL-J Series family of message formats shall be used for information transfer with systems and/or weapons platforms that use a Joint Tactical Data Link. This series of message formats are a family of common data element structures based on TADIL-J message formatting that incorporates elements of other formats: VMF, TADILs J & K, Link 22, and Link 16. TADIL-J message formats or Joint VMF message formats can be used as a migration standard until the J Series family of message formats has completely matured. TADIL-J message formats are specified in the *Joint Tactical*

Information Distribution System (JTIDS) TIDP Test Edition. Joint VMF message formats are specified in the *Joint VMF TIDP*.

4.2.4.5 Remote Procedure Calls

The Distributed Computing Environment (DCE) provides the capability to exchange standard data among heterogeneous platforms, DBMS and legacy data structures using Remote Procedure Calls (RPCs). Interfaces of this type can be defined using the DCE Interface Definition Language (IDL) but must use applicable data elements from the DDDS. See Section 2.2.2.2.4 for specific standards.

4.2.4.6 Data Exchange Emerging Standards

The Army with DISA JIEO is working to develop the strategy and policy for migration from the current multiple bit-oriented and character-oriented tactical data link message formats to a minimal family of DOD 8320.1 compliant information exchange standards. A normalized unified data/message element dictionary will be developed based on the Enterprise Data Model (EDM) and associated data element standards. The dictionary will support both character and bit-oriented representation of the standard data and their domain values. Message standards will then establish the syntax for standard data packaging to support mission requirements (e.g., character or bit-oriented, fixed or variable format, etc.). The unified data dictionary will ensure that multiple representations are minimized and transformation algorithms are standardized.

JTIDS will soon be replaced by the Multifunctional Information Distribution System (MIDS). Message format standards for MIDS will not change from those of the JTIDS. Message and data element standards must be independent of the information transport standards, protocols and profiles. Refer to section 3 of this document for information transport standards.

4.2.5 Modeling and Simulation Information and Data Exchange Standards

Refer to Appendix G for information standards, both mandated and emerging, that are unique to the modeling and simulation domain.

This page was intentionally left blank.

SECTION 5

HUMAN COMPUTER INTERFACES

5.1 INTRODUCTION

5.1.1 Purpose

This section provides a common framework for Human-Computer Interface (HCI) design and implementation in Army automated systems. The objective is to standardize user interface design and implementation options thus enabling Army applications within a given domain to appear and behave consistently. The standardization of HCI appearance and behavior within the Army will result in higher productivity, shorter training time, and reduced development, operation, and support costs. This section specifies HCI design guidance, mandates, and standards.

5.1.2 Scope

This section applies to the human interface of automated systems described in Paragraph 1.1.3. This version mandates the design of graphical and character-based displays and controls for Army automated systems.

5.1.3 Background

The objective of system design is to ensure system reliability and effectiveness. To achieve this objective the human must be able to interact effectively with the system. Humans interact with automated systems using the HCI. The HCI includes the appearance and behavior of the interface, physical interaction devices, graphical interaction objects, and other human-computer interaction methods. A good HCI is both easy to use and appropriate to the operational environment. It exhibits a combination of user-oriented characteristics such as intuitive operation, ease and retention of learning, facilitation of user task performance, and consistency with user expectations.

The need to learn the appearance and behavior of different system HCIs increases both the training burden and the probability of operator error. What is required are interfaces that exhibit a consistent appearance and behavior both within and across applications and systems.

5.2 MANDATES

5.2.1 General

The predominant types of HCIs include graphical user interfaces (GUIs) and character-based interfaces. For all DOD automated systems, the near-term goal is to convert character-based interfaces to a GUI. Although GUIs are the preferred user interface, some specialized interfaces (e.g., embedded/weapons systems) may require use of character-based or alternative interfaces due to operational, technical, or physical constraints. These specialized interfaces shall be defined by domain-level style guides and further detailed in system-level user interface specifications. However, graphical and character-based interface styles shall not be mixed within the same system or family of systems.

5.2.1.1 Graphical User Interfaces

Graphical user interfaces for Army automated systems shall be based on a commercial user interface style in accordance with paragraph 5.2.2.1. Hybrid GUIs that mix user interface styles (e.g., Motif with Windows) shall not be created.

Developers shall investigate use of a commercial GUI style, or subset thereof, before developing a custom GUI. Operational, technical, or physical constraints associated with certain types of systems (e.g., embedded/weapons systems) may not permit the use of a commercial GUI style. If a non-commercial GUI is necessary as the basis for the HCI, developers shall provide detailed justification and receive approval before proceeding with development.

5.2.1.2 Character-based Interfaces

Systems with an approved requirement for a character-based interface shall comply with the character-based interface design criteria contained in the *DOD HCI Style Guide*.

While not mandated, additional guidance for developing character-based interfaces can be found in ESD-TR-86-278, *Guidelines for Designing User Interface Software* (Smith and Mosier 1986).

5.2.1.3 MIL-STD-2525, Common Warfighting Symbology

MIL-STD-2525, C*ommon Warfighting Symbology,* Version 1, 30 September 1994, prescribes a set of common warfighting symbols along with basic application and display rules for DOD operations, system development, and training. This interim standard is mandated by DOD within the context of warfighting operations. If no symbol is available in MIL-STD-2525 to meet system requirements, developers shall submit a candidate symbol for inclusion in the next version of MIL-STD-2525.

5.2.1.4 Security

The HCI shall comply with Section 6 of the Army Technical Architecture; Appendix A, Security Presentation Guidelines, DOD HCI Style Guide; and other applicable portions of the DOD HCI Style Guide.

5.2.2 Style Guides

Figure 5-1 illustrates the hierarchy of style guides that shall be followed to maintain consistency and good HCI design within the Army. This hierarchy, when applied according to the HCI design process mandated in the DOD HCI Style Guide, provides a framework that supports iterative prototype-based HCI development. The process starts with top-level general guidance and uses prototyping activities to develop system-specific design rules.

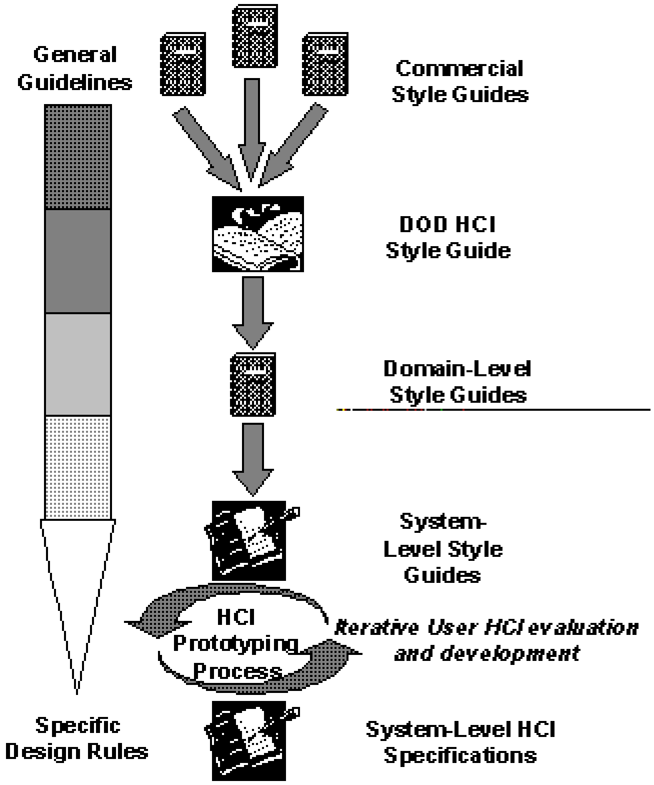

General Guidelines
Commercial Style Guides
DOD HCI Style Guide
Domain-Level Style Guides
System-Level Style Guides
HCI Prototyping Process
Iterative User HCI evaluation and development
Specific Design Rules
System-Level HCI Specifications

FIGURE 5-1. HIERARCHY OF STYLE GUIDES

The interface developer shall use the selected commercial GUI style guide, refinements provided in the *DOD HCI Style Guide,* and the appropriate domain-level style guide, as well as input from human factors specialists, to create the system-specific HCI. The following paragraphs include specific guidance regarding the style guide hierarchy levels.

5.2.2.1 Commercial Style Guides

A commercial GUI style shall be selected as the basis for user interface development. The GUI style selected is usually driven by the mandates specified in Section 2 (User Interface Services and Operating System Services). The following commercial GUI style guide is mandated.

- *Open Software Foundation (OSF)/MotifTM Style Guide, Revision 1.2* (OSF 1992).

OSF/Motif is a non-proprietary interface style that supports the DOD goal for an open systems environment. Use of non-commercial GUI styles is addressed in paragraph 5.2.1.1.

5.2.2.2 DOD HCI Style Guide

The DOD HCI Style Guide, Volume 8 of the TAFIM, was developed as a guideline document presenting recommendations for good human computer interface design. This document focuses on human computer behavior and concentrates on elements or functional areas that apply to DOD applications. These functional areas include such things as security classification display, mapping display and manipulation, decision aids, and embedded training. This style guide, while emphasizing commercial GUIs, contains interface design criteria that can be used for all types of systems including those which employ character-based interfaces.

Although the *DOD HCI Style Guide* is not intended to be strictly a compliance document, it does represent DOD policy. Army systems shall therefore conform to the interface design criteria contained in the *DOD HCI Style Guide.*

Although the general principles given in this document apply to all interfaces, some specialized areas require separate consideration. Specialized interfaces, such as those used in real time weapon system applications, have interface requirements that are beyond the scope of the *DOD HCI Style Guide.* These systems shall comply with their domain-level style guide and follow the general principles and HCI design guidelines presented in the *DOD HCI Style Guide*.

5.2.2.3 Domain-level Style Guides

A domain-level HCI style guide shall be developed by each approved domain within the Army. These style guides will reflect the consensus on HCI appearance and behavior for a particular domain (e.g., C3I) within the Army. The domain-level style guide will be the compliance document and may be supplemented by a system-level style guide created as an appendix to the domain-level style guide.

C3I is the only domain that currently has a domain-level style guide. Until a domain develops their domain-level style guide, they shall comply with paragraph 5.2.2.2 above and the *User Interface Specifications for the GCCS.* Non-C3I domains are encouraged to adopt all or applicable parts of the *User Interface Specifications for the GCCS* as the basis for their domain-level style guides.

5.2.2.4 System-level Style Guides

System-level style guides provide the special tailoring of commercial, DOD, and domain-level style guides. These documents include explicit design guidance and rules for the system while maintaining the appearance and behavior provided in the domain-level style guide. If needed, the system-level style guide will be created as an appendix to the applicable domain-level style guide. The system-specific appendix will specify unique requirements not addressed in the domain-level style guide.

5.3 EMERGING USER INTERFACE STYLES

The Army Technical Architecture mandates the development of a domain-level HCI style guide for each approved domain within the Army. Currently, a domain-level style guide exists for the C3I domain. Efforts are underway to develop domain-level style guides for other domains. These emerging domain-level style guides will be mandated for use when they are completed, coordinated across domains, and approved.

The *User Interface Specification for the GCCS Version 1.0* will be superseded in calendar year 1996 by the *User Interface Specification for the Defense Information Infrastructure (DII) Version 1.0*. The DII specification will be an umbrella specification for both command and control systems and combat support systems. It will be the equivalent to Version 1.1 of the GCCS specification and include Microsoft Windows design guidance.

MIL-STD-2525, Version 1, is an interim standard. It requires the use of supplemental standards to provide the warfighter a comprehensive set of symbology. Version 2 will expand the existing symbology set and is expected to be mandated in late 1996.

Currently, research is underway to investigate non-traditional user interfaces. Such interfaces may be gesture-based and may involve processing multiple input sources, such as voice and spatial monitors. Ongoing research and investigation include the use of virtual reality and interface agents. Interface agents autonomously act on behalf of the user to perform various functions, thus allowing the user to focus on the control of the task domain. The Army will integrate standards for non-traditional user interfaces as research matures and commercial standards are developed.

This page was intentionally left blank.

SECTION 6

INFORMATION SECURITY

6.1 INTRODUCTION

6.1.1 Purpose

This section describes the information security standards that apply to Army systems that produce, use or exchange information electronically. These standards provide the warfighter with a seamless flow of timely, accurate, **accessible**, and **secure** information.

6.1.2 Scope

The standards described in this section are drawn primarily from formally developed national and international standards. In order to be effective, security standards must be integrated into and used with the other information standards in the ATA. Therefore this section is structured to mirror the structure of the ATA itself with security standards organized corresponding to each ATA section. An additional subsection has been provided to address security unique considerations. This section assumes a level of knowledge of information security above an operational level.

6.1.3 Background

The TAFIM provides a blueprint for the Defense Information Infrastructure (DII), capturing the evolving vision of a common, multipurpose, standards-based technical infrastructure. The DOD Goal Security Architecture (DGSA), Volume 6 of the TAFIM, provides a comprehensive view of the architecture from the security perspective. The DGSA is a generic architectural framework for developing mission specific security architectures. The DGSA provides the basis of the security standards discussion in this section of the ATA. While the DGSA is oriented toward future systems, today's technology and standards can be used to achieve DGSA-consistent systems that are on the path to complete implementation of the DGSA.

Systems that process sensitive data must be certified and accredited before use. Certification is the technical evaluation of an Automated Information System's (AIS's) security features and other safeguards, made in support of the accreditation. Accreditation is the authorization by the Designated Approving Authority (DAA) that an automated system may be placed into operation. Therefore, system developers should open dialog with the DAA concurrently with their use of the ATA, as DAA decisions can affect the applicability of standards within specific environments.

Security requirements and engineering should be determined in the initial phases of design. The determination of security services to be used and the strength of the mechanisms providing the services are primary aspects of developing the specific security architectures to support specific domains. Section 6 of the ATA is used after operational architectural decisions are made regarding the security services needed and the required strengths of protection of the mechanisms providing those services. Section 6 of the ATA can also be used to assess the relevance of standards that can be met with evaluated commercial and government-provided components and protocols. The ATA can be used as a tool to evaluate elements of the system architecture regarding operational security requirements, standards compliance, interoperability with other systems, and cost reduction through software reuse.

Other technical architectural decisions must be made after considering Army enterprise level regulations. AR 380-19, Information System Security, contains the necessary references to other standards and mandates that must be considered by a system developer. Comprehensive system and security engineering are the basis for selecting proper combinations of standards to develop a system that meets the needs of mission security requirements.

6.2 INFORMATION PROCESSING SECURITY STANDARDS

Information processing security services are defined in ISO 7498-2. These services include authentication, access control, data integrity, data confidentiality, non-repudiation and availability. Availability management is not included in this international standard but is specifically called out in the DGSA for the local communications system and communications network management facilities. ISO 10181, OSI Security Frameworks, extends this list of services by including security audit and key management.

As a general requirement, all Army systems must demonstrate that they meet the applicable security profile described in both AR 380-19 and the DOD Trusted Computer System Evaluation Criteria standard, DOD 5200.28-STD.

6.2.1 Mandated Standards

6.2.1.1 Application Software Entity

DOD has mandated the use of Multilevel Information System Security Initiative (MISSI) products for DOD managed systems. The various specifications and types of products available that implement the security services are identified in the MISSI Implementation Guide. One of the products is the FORTEZZA card, a PC card (formerly known as a PCMCIA card) that provides several security services for electronic mail. Some security functions that would normally be invoked by applications are described in 6.3.1.1.1. The interface to the FORTEZZA card is described in:

- FORTEZZA Interface Control Document, Revision P1.5, 22 Dec 1994, FOUO.
- FORTEZZA Plus Interface Control Document, Release 3.0, 1 June 1995, FOUO.

Evaluation Criteria Standards, which describe security designations such as C2, B1, etc. are contained in:

- DOD 5200.28-STD, The Department of Defense Trusted Computer System Evaluation Criteria, DOD 5200.28-STD, GPO 1986-623-963,643-0, December 1985 with interpretations.
- NCSC-TG-021, Version-1, Trusted Database Management System Interpretation, April 1991.

6.2.1.2 Application Platform Entity

Army systems that are required to exchange information at multiple sensitivity levels require a standard labeling format to identify the sensitivity level of the information. The following labeling standard applies:

- DOD Intelligence Information Systems (DODIIS) Network Security for Information Exchange (DNSIX), (Defense Intelligence Agency (DIA), DDS-2600-5984-01, DDS 2600-5985-91).

Security Alarm Reporting:

- ISO/IEC 10164-7, 1992, Information Technology-Open System Interconnection - Systems Management - Part 7: Security Alarm Reporting Function, ISO/IEC JTC1 SC21/WG4, IS May 1992 (ITU-T X.736, 1992) (Security management/systems management/programming interface).
- IEEE 1003.6, POSIX Security Enhancements.

Evaluation Criteria Standard:

- DOD 5200.28-STD, The Department of Defense Trusted Computer System Evaluation Criteria, DOD 5200.28-STD, GPO 1986-623-963,643-0, December 1985.

6.2.2 Emerging Standards

6.2.2.1 Application Software Entity

FORTEZZA provided security services for functions other than electronic mail are still emerging and are not yet mandated. However, systems should strongly consider the possibility of a mandate in the near future.

General Security In Open Systems:

- ISO/IEC DII 10181 Series, Information Technology - Open Systems Interconnection -Security Frameworks in Open Systems, 1994 - 1995.

Generic Data Unit Protection API:

Applications such as secure electronic mail where data needs to be protected without any on-line connection with the intended recipient(s) of that data could make use of a generic security service. Subsequent to being protected, the data unit can be transferred to the recipient(s) - or to an archive - perhaps to be processed as unprotected only days or years later. The IDUP-GSS-API extends the GSS-API [RFC-1508] for non-session protocols and applications requiring protection of a generic data unit (such as a file or message) in a way which is independent of the protection of any other data unit and independent of any concurrent contact with designated "receivers" of the data unit.

- Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API), 07/06/1995.

6.2.2.2 Application Platform Entity

- DII 10164-9, SC21 N9390, Information Technology - Open System Interconnection - Systems Management - Part 9: Objects and Attributes for Access Control (final text).

Firewalls:

The use of network firewalls, systems that effectively isolate an organization's internal network structure from an exterior network such as the Internet, are becoming increasingly popular. These firewall systems typically act as application-layer gateways between networks, usually offering controlled TELNET, FTP, and SMTP access. With the emergence of more sophisticated application layer protocols designed to facilitate global information discovery, there exists a need to provide a general framework for these protocols to transparently and securely traverse a firewall. This Internet draft defines this framework.

- SOCKS Protocol Version 5, 10/04/1995.

There are Internet draft specifications for additional security services for SOCKS:

- Username/Password Authentication for SOCKS V5, 05/30/1995.
- GSS-API Authentication Method for SOCKS Version 5, 07/05/1995.

6.2.2.3 Remote Authentication

Remote Authentication Dial In User Service (RADIUS), et. al., May 1995. This Internet draft describes a protocol for carrying authentication, authorization, and configuration information between a Network Access Server that desires to authenticate its links and a shared Authentication Server.

6.2.2.4 Security Extensions

"FTP Security Extensions", M. Horowitz, S. Lunt, 07/07/1995. This Internet draft defines extensions to the "FILE TRANSFER PROTOCOL (FTP)" specification RFC 959, (October 1985). These extensions provide strong authentication, integrity, and confidentiality on both the control and data channels with the introduction of new optional commands, replies, and file transfer encoding. The following new optional commands are introduced in this specification: AUTH (Authentication Mechanism), ADAT (Authentication Data), PROT (Data Channel Protection Level), PBSZ (Protection Buffer Size), CCC (Clear Command Channel), MIC (Integrity Protected Command), CONF (Confidentiality Protected Command), and ENC (Privacy Protected Command). A new class of reply types (6yz) is also introduced for protected replies. None of the above commands are required to be implemented, but interdependencies exist. These dependencies are documented with the commands. Note that this specification is compatible with RFC 959.

6.2.2.5 Generic Security Service Application Program Interface (GSS API)

The Generic Security Service Application Program Interface (GSS-API) [RFC 1508], Sept. 1993 definition provides security services to callers in a generic fashion, supportable with a range of underlying mechanisms and technologies and hence allowing source-level portability of applications to different environments. This specification defines GSS-API services and primitives at a level independent of underlying mechanism and programming language environment, and is to be complemented by other, related specifications:

- Documents defining specific parameter bindings for particular language environments.
- Documents defining token formats, protocols, and procedures to be implemented in order to realize GSS-API services atop particular security mechanisms.

6.2.2.6 Security Management Protocol

Progress toward approval of SNMP V2 has been slow. In the meantime CMIP has been adopted by many developers for the management of circuit-switched systems. It is envisioned that a future Network and System Management standard will incorporate features of both SNMP V2 and CMIP for packet-switched and circuit-switched environments respectively. Developers should build or use products that are based on these standards to the maximum extent possible.

- ISO/IEC 9596-1, 1991, Information Technology - Open Systems Interconnection - Common Management Information Protocol (CMIP) - Part 1: Specification (includes Amendments 1 and 2 of 9596-1, 1990), ISO/IEC JTC1 SC21/WG4, IS June 1991 (ITU-T X.711, 1991) (constrained dispersion/transfer system/network security protocols; security management/systems management/security management protocols).

- ISO/IEC 10736m 199X, SC6 N8455, Information Technology - Open Systems Interconnection - Transport Layer Security Protocol Plus Amendment 1 on Security Association Establishment Protocol, ISO/IEC JTC1 SC6/WG4, IS 1994 (ITU-T X.274) (constrained dispersion/transfer system/network security protocols; security management/systems management/security management protocols).

- IEEE 802.10c/D6 Standard for Interoperable LAN Security-Part C: Key Management, IEEE, Draft 6 issued 1994; draft 7 in-process, (security management/key management/protocols).

- IEEE 802.10d, Standard for Interoperable LAN Security-Part D: Security Management, IEEE, on hold, (layer 7 protocol to securely manage the security protocols).

6.2.2.7 Other

- Security Architecture for the Internet Protocol (RFC 1825).

- IP Authentication Header (RFC 1826).

- IP Encapsulating Security Payload (ESP) (RFC 1827).

- The ESP DES-CBC Transform (RFC 1829).

- IP Authentication using Keyed MD5 (RFC 1828).

- ISO/IEC 10021-1, 1990/DAM 4, Information Technology-Message Handling Systems (MHS)-Part 1: System and Service Overview-Amendment 4: Interpersonal Messaging Security Extensions, ISO/IEC JTC1 SC18/WG4, IS 1990 (ITU-T X.400).

- ISO/IEC 11577, 199X, SC6 N8453, Information Technology-Telecommunications and Information Exchange Between Systems-Network Layer Security Protocol, ISO/IEC JTC1 SC6/WG2, IS June 1994, (ITU-T X.273) (constrained dispersion/transfer system/network security protocols).

- ISO/IEC 10736, 199X, SC6 N8455, Information Technology-Open Systems Interconnection-Transport Layer Security Protocol Plus Amendment 1 on Security Association Establishment Protocol, ISO/IEC JTC1 SC6/WG4, IS 1994, (ITU-T X.274) (constrained dispersion/transfer system/network security protocols; security management/systems management/security management protocols).

- IEEE 802.10, IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS), IEEE, 1992, (Services, protocols, data formats, interfaces to allow IEEE 802 products to interoperate, authentication, access control, data integrity, and confidentiality).

- IEEE 802.10a, Standard for Interoperable LAN Security-The Model, IEEE, Draft Jan 1989, (Shows relationship of SILS to OSI. Describes required interfaces.).

- IEEE 802.10b, Standard for Interoperable LAN Security-Part B: Secure Data Exchange, IEEE, 1992, (Secure data exchange at the data link layer).

6.3 INFORMATION TRANSPORT SECURITY STANDARDS

This section discusses the security standards that have an impact on the information transport security services.

6.3.1 MANDATES

6.3.1.1 MISSI

The DOD has mandated the MISSI for the protection of the DII.

6.3.1.1.1 MISSI Cryptographic Algorithms

MISSI's current FORTEZZA card includes a CAPSTONE chip containing a time stamping capability and four algorithms. The algorithms can be found in FIPS PUB 180, National Institute of Standards and Technology (NIST) Secure Hash Algorithm (SHA) (NIST;11 May 1993); FIPS PUB 186, NIST Digital Signature Standard (DSS) algorithm (NIST; 19 May 1994); NSA-developed Type II confidentiality algorithm (SKIPJACK); and NSA-developed Type II Key Exchange Algorithm (KEA). The following API governs the interface to the services of the FORTEZZA card.

- FORTEZZA Cryptologic Interface Programmers Guide for the Fortezza Crypto Card, Version 1.51, 15 May 1995.

Design of the operating system drivers and/or hardware adapters to use the resources provided by the FORTEZZA card need the technical detail contained in the Interface Control Document (ICD). For the card, this can be found in the ICD for the FORTEZZA Crypto Card, Version P1.5, 22 December 1994.

For those systems that need to escrow an encryption key, the following standard applies:

- FIPS PUB 185, NIST, 9 February 1994, Escrowed Encryption Standard.

6.3.1.1.2 MISSI Security Protocols

Security protocols that are algorithm independent, such as Message Security Protocol (MSP) and NLSP, can readily take advantage of these algorithms. Many of the protocols developed under the Secure Data Network System (SDNS) program and published under NIST in report NISTIT 90-4250, have become part of MISSI. MISSI currently uses MSP for messaging, Key Management Protocol (KMP), and Security Protocol at Layer 3 (SP3). SP3 is used in two MISSI products, the Tactical End-to-End Encryption Device (TEED) and the Network Encryption System (NES). Additionally, MISSI has recently added FIPS PUB JJJ, as its identification and authentication (I&A) protocol.

6.3.1.1.3 MISSI Digital Signature Infrastructure

Wide-spread use of MISSI is dependent upon the successful establishment of a certificate and key management infrastructure. This infrastructure is responsible for the proper creation distribution and revocation of the end user's public key certificates. These certificates are based on ITU-T Rec. X.500 (ISO/IEC 9594-1) Directory Infrastructure and ITU-T Rec. X.509 Version 3 Authentication Certificates.

Until the planned DMS X.500 directory infrastructure components are in place, developers must use an interim non-standard local caching system.

6.3.1.2 Transport Mechanisms

- NCSC-TG-005, Version-1, Trusted Network Interpretation, July 1987.

6.3.2 Emerging Standards

6.3.2.1 Security Association Management

- ISP-421/94.05.15 Revision 1.0: The ISDN Security Program (ISP) Security Association Management Protocol (SAMP).

6.3.2.2 World Wide Web (WWW)

While EDI is the current DOD mandated mechanism for electronic commerce and will probably continue to be supported by industry for large volume, commodity-type procurements at the wholesale level, the commercial marketplace has adopted Secure-HTTP (S-HTTP) for retail purchases over a public InterNetwork. EDI requires translation software to convert business application information into an EDI information standard. A common standard in the United States is the ANSI X.12 EDI format.

S-HTTP is an extension of Hypertext Transfer Protocol (HTTP), which forms the basis for the World Wide Web. S-HTTP, Version 1.1, provides independently applicable security services for transaction confidentiality, authenticity/integrity and non-reputability of origin. The design intent is to provide a flexible protocol that supports multiple orthogonal operation modes, key management mechanisms, trust models, cryptographic algorithms and encapsulation formats, all through option negotiation between parties for each transaction.

While there is a virtual consensus on the S-HTTP protocol itself, there are several competing schemes for encryption. The two predominant and totally incompatible approaches are Netscape's Secure Courier and Microsoft's Secure Transaction Technology. Both of these schemes use the same Secure Sockets Layer (SSL) encryption scheme.

Two Internet Drafts for SSL and S-HTTP are being considered for standardization:

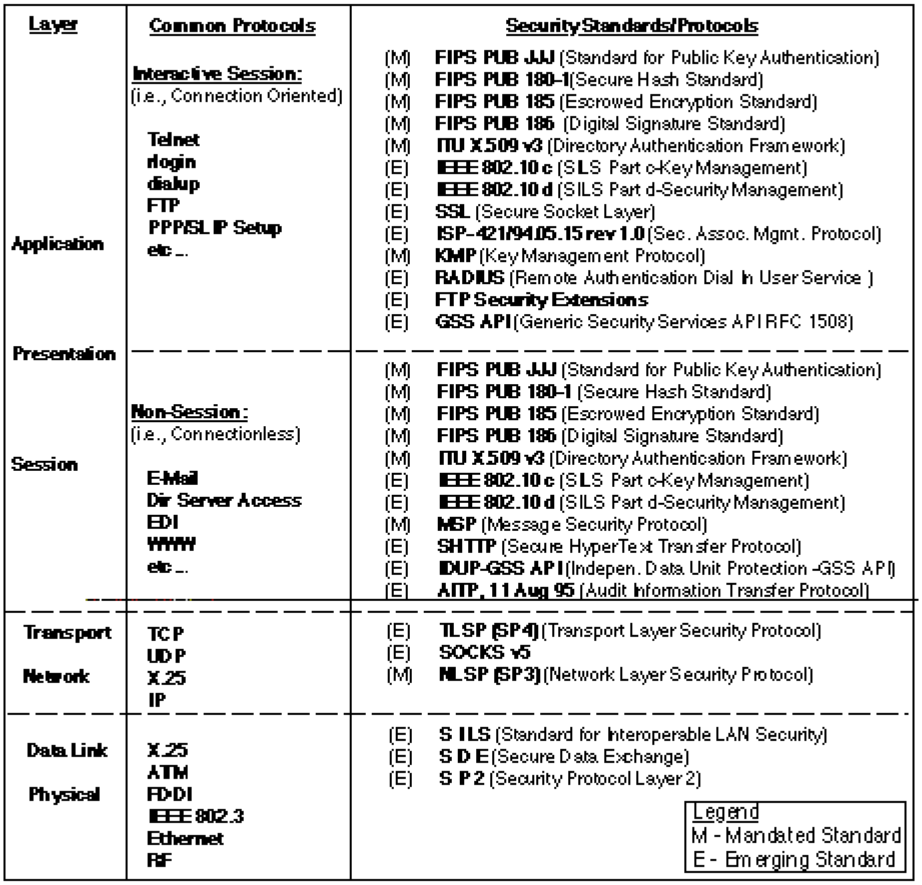
- For SSL, Internet Draft June 95 - Dec 95, Version 3.
- For S-HTTP, Internet Draft July 95 - Jan 96.

6.3.3 Summary of Standards

Table 6-1 shows a mapping of common protocols and security standards and protocols that may be used to provide the required security services. International

Organization for Standardization (ISO) 7498-2 Security Service Recommendations (1989), provides a list of applicable security services and makes recommendations for their implementation.

TABLE 6-1 PROTOCOLS AND SECURITY STANDARDS



Layer	Common Protocols	Security Standards/Protocols
Application Presentation Session	**Interactive Session:** (i.e., Connection Oriented) **Telnet** **rlogin** **dialup** **FTP** **PPP/SLIP Setup** **etc ...**	(M) **FIPS PUB JJJ** (Standard for Public Key Authentication) (M) **FIPS PUB 180-1**(Secure Hash Standard) (M) **FIPS PUB 185** (Escrowed Encryption Standard) (M) **FIPS PUB 186** (Digital Signature Standard) (M) **ITU X.509 v3** (Directory Authentication Framework) (E) **IEEE 802.10 c** (SLS Part c-Key Management) (E) **IEEE 802.10 d** (SILS Part d-Security Management) (E) **SSL** (Secure Socket Layer) (E) **ISP-421/94.05.15 rev 1.0** (Sec. Assoc. Mgmt. Protocol) (M) **KMP** (Key Management Protocol) (E) **RADIUS** (Remote Authentication Dial In User Service) (E) **FTP Security Extensions** (E) **GSS API** (Generic Security Services API RFC 1508)
	Non-Session: (i.e., Connectionless) **E-Mail** **Dir Server Access** **EDI** **WWW** **etc ...**	(M) **FIPS PUB JJJ** (Standard for Public Key Authentication) (M) **FIPS PUB 180-1** (Secure Hash Standard) (M) **FIPS PUB 185** (Escrowed Encryption Standard) (M) **FIPS PUB 186** (Digital Signature Standard) (M) **ITU X.509 v3** (Directory Authentication Framework) (E) **IEEE 802.10 c** (SLS Part c-Key Management) (E) **IEEE 802.10 d** (SILS Part d-Security Management) (M) **MSP** (Message Security Protocol) (E) **SHTTP** (Secure HyperText Transfer Protocol) (E) **IDUP-GSS API** (Indepen. Data Unit Protection -GSS API) (E) **AITP, 11 Aug 95** (Audit Information Transfer Protocol)
Transport Network	**TCP** **UDP** **X.25** **IP**	(E) **TLSP (SP4)** (Transport Layer Security Protocol) (E) **SOCKS v5** (M) **NLSP (SP3)** (Network Layer Security Protocol)
Data Link Physical	**X.25** **ATM** **FDDI** **IEEE 802.3** **Ethernet** **RF**	(E) **S ILS** (Standard for Interoperable LAN Security) (E) **S D E** (Secure Data Exchange) (E) **S P 2** (Security Protocol Layer 2) Legend M - Mandated Standard E - Emerging Standard

The appropriate security services required for any Army system must be determined during that system's security engineering process. This process must be closely coordinated with the system's designated approving authority (DAA), who will be cognizant of the germane security policies.

6.4 INFORMATION MODELING AND DATA EXCHANGE SECURITY STANDARDS

The DGSA discusses the need for a separation mechanism to mediate all calls to security critical functions and ensure strict isolation is maintained. A security management information base (SMIB) will contain the description of objects that are managed by the separation mechanism. However, the object class definitions for managing critical security functions are not currently standardized. Therefore, standards identified in the two following sections are provided for information and migration planning but are NOT mandated for use.

6.4.1 Mandated Standards

None mandated at this time.

6.4.2 Emerging Standards

- ISO/IEC 10165 Series, Information Technology - Open Systems Interconnection - Structure of Management Information - Parts 1- 4, 1993 - 1994.
- DII 10164-9, SC21 N9390, Information Technology - Open Systems Interconnection - Systems Management - Part 9: Objects and Attributes for Access Control (Final Text), ISO/IEC JTC1 SC21/WG4, DII April 1993, target IS Mar. 1994 (ITU-T X.741) (strict isolation/security critical functions/elements of management information; decision and enforcement separation/separation policy representation/elements of management information; constrained dispersion/transfer system/security information objects, elements of management information; security management/systems management/elements of management information).

6.5 HUMAN-COMPUTER INTERFACE SECURITY STANDARDS

One aspect of the human-computer interface is the need to identify individual users of an end system. End systems in turn need to be able to authenticate remote entities whether they are users, other end systems, or relay systems. The standards listed below identify the existing techniques for authentication. Specific selection of a standard should be mission specific.

6.5.1 Mandated Standards

6.5.1.1 Security Banners and Screen Labels

- Department of Defense (DOD). 1994b. *Department of Defense Human Computer Interface Style Guide* (Version 2.0), Defense Information Systems Agency Center for Information Management, McLean, Virginia.

6.5.2 Emerging Standards

6.5.2.1 Entity Authentication

- ISO/IEC 9798-1, 1991, Entity Authentication Mechanisms, Part 1- 4: General Model, ISO/IEC JTC1 SC27/WG2, 1991 - 1995, (strict isolation/protection mechanisms/techniques).

6.5.2.2 Personal Authentication

- WD 9798-5, SC27 N 1104 (Project 1.27.03.05), Entity Authentication Mechanisms - Part 5: Entity Authentication Using Zero Knowledge Techniques, ISO/IEC JTC1 SC27/WG2, WD, target CD 1995, DII 1996, and IS 1997.

6.6 SECURITY RELATED DOCUMENTS

While most system planners and architects look to standards to arrive at a basic set of requirements, systems security is driven by policy. Security policy appears at many levels, including federal laws (e.g., The Privacy Act) and policy for the handling of national intelligence information (e.g., DCID 1/16). Such policies do not have directly associated standards, yet their compliance requirements can affect both the system and technical architectures.

For those systems required or desiring to use a cryptographic device to protect privacy act information and other, unclassified, non-Warner Act exempt information, the Data Encryption Standard (DES) may apply. The DES is found in FIPS PUB 46-2 Data Encryption Standard, December 1993.

The C2 Protect initiative addresses those measures taken to maintain effective C2 of U.S. Army forces. While there are no technical standards mandated, it does establish a library of tasks and actions necessary to implement, manage, and support the initiative.

APPENDIX A - ACRONYMS

AAL	ATM Adaptation Layer
ABCS	Army Battle Command System
ACCS	Army Command and Control System
ACM	Association of Computing Machinery
ACP	Allied Communication Publication
ACT	Advanced Concept and Technology
ACTD	Advanced Concept Technology Demonstration
ADDS	Army Data Distribution System
ADDSI	ADDS Interface
ADO	Army Digitization Office
ADP	Automated Data Processing
AFATDS	Advanced Field Artillery Tactical Data System
AGCCS	Army Global Command and Control System
AIS	Automated Information Systems
AITP	Audit Information Transfer Protocol
ALSP	Aggregate Level Simulation Protocol
AMHS	Automated Message Handling System
ANSI	American National Standards Institute
API	Application Programming Interface
AR	Army Regulation
ARC	Arc Second Raster Chart
ARP	Address Resolution Protocol
ARPA	Advanced Research Projects Agency
AS	Autonomous System
ASAS	All Source Analysis System
ASB	Army Science Board
ASCII	American National Standard Code for Information Interchange
ASD	Assistant Secretary of Defense
ATA	Army Technical Architecture
ATD	Advanced Technology Demonstration
ATM	Asynchronous Transfer Mode
B2C2	Brigade and Below Command and Control
BGP	Border Gateway Protocol
BOOTP	Bootstrap Protocol
BOS	Battlefield Operating System
BRI	Basic Rate Interface
C2	Command and Control
C2	Class C2 (from DOD 5200-28-STD)

C4	Command, Control, Communications, and Computers
C2V	Command and Control Vehicle
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Computers, and Intelligence
C2CDM	C2 Core Data Model
CAD	Computer-Aided Design
CADRG	Compressed ARC Digitized Raster Graphics
CASE	Computer Aided Software Engineering
CCITT	International Telephone and Telegraph Consultative Committee (now ITU-T)
CDE	Common Desktop Environment
CGI	Computer Generated Imagery
CGM	Computer Graphics Metafile
CIB	Controlled Image Base
CINC	Commander-in-Chief
CMIP	Common Management Information Protocol
CMMS	Conceptual Models of the Mission Space
CNR	Combat Net Radio
COE	Common Operating Environment
CONUS	Continental United States
CORBA	Common Object Request Broker Architecture
COS	Corporation for Open Systems
COSE	Common Open Software Environment
COTS	Commercial Off-the-Shelf
CSC	Computer Security Center
CSMA/CD	Carrier Sense Multiple Access / Collision Detection

DAA	Designated Approving Authority
DBMS	Database Management System
DCE	Distributed Computing Environment
DCE	Data Circuit-Terminating Equipment
DCID	Director of Central Intelligence Directive
DCPS	Data Communications Protocol Standard
DDDS	Defense Data Dictionary System
DDN	Defense Data Network
DDRS	Defense Data Repository System (now DDDS)
DDS	Directorate of Information Services
DES	Data Encryption Standard
DGSA	DOD Goal Security Architecture
DHCP	Dynamic Host Configuration Protocol
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DIS	Distributed Interactive Simulation

DISA	Defense Information Systems Agency
DISC4	Director of Information Systems for Command, Control, Communications, and Computers
DISN	Defense Information Systems Network
DISSP	Defense Information Systems Security Program
DMA	Defense Mapping Agency
DMS	Defense Message System
DNC	Digital Nautical Chart
DNS	Domain Name System
DNSIX	DODIIS Network Security for Information Exchange
DOD	Department of Defense
DODD	Department of Defense Directive
DODIIS	Department of Defense Intelligence Information Systems
DOS	Disk Operating System
DSS	Digital Signature Standard
DTE	Data Terminal Equipment
DTED	Digital Terrain Elevation Data
DTLOMS	Doctrine, Training, Leader Development, Organization, Materiel, and Soldiers
DTMP	DCPS Technical Management Panel

EDI	Electronic Data Interchange
EDM	Enterprise Data Model
EEI	External Environment Interface
EIA	Electronics Industries Association
EPS	Encapsulated PostScript
ESP	Encapsulating Security Payload

FAAD	Forward Area Air Defense
FBCB2	Force XXI Battle Command Brigade and Below
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standards
FOUO	For Official Use Only
FTP	File Transfer Protocol

GCCS	Global Command and Control System
GCSS	Global Combat Support System
GIF	Graphics Interchange Format
GKS	Graphical Kernel System
GOTS	Government Off-the-Shelf
GPS	Global Positioning System
GSS	Generic Security Service

GUI	Graphical User Interface
HCI	Human-Computer Interface
HF	High Frequency
HLA	High Level Architecture
HQDA	Headquarters Department of the Army
HTI	Horizontal Technology Integration
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
I&A	Identification & Authentication
I&RTS	Integration & Runtime Specification
IAB	Internet Architecture Board
IAW	In Accordance With
ICCCM	Inter Client Communications Convention Manual
ICD	Interface Control Document
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IEW	Intelligence/Electronic Warfare
ICMP	Internet Control Message Protocol
ICOM	Inputs, Controls, Outputs, and Mechanisms
IDEF	Integrated Computer Aided Manufacturing Definition
IDEF0	Integrated Computer Aided Manufacturing Definition Function Method
IDEF1X	Integrated Computer Aided Manufacturing Definition Extended Data Method
IDL	Interface Definition Language
IDUP	Independent Data Unit Protection
IEEE	Institute of Electrical and Electronic Engineers
IGES	Initial Graphics Exchange Specification
IGMP	Internet Group Management Protocol
IGOSS	Industry/Government Open Systems Specification
INC	Interface Network Controller
INFOSEC	Information System Security
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	ISDN Security Program
IT	Information Technology
ITU	International Telecommunications Union
IXMP	Information Standards Management Panel

JCS	Joint Chiefs of Staff
JIEO	Joint Interoperability and Engineering Organization
JMCIS	Joint Maritime Command Information System
JPEG	Joint Picture Expert Group
JRSC	Jam Resistant Secure communications
JTIDS	Joint Tactical Information Distribution System

KEA	Key Exchange Algorithm
KMP	Key Management Protocol

LAN	Local Area Network
LANE	Local Area Network Emulation
LAPB	Link Access Protocol Balanced
LLC	Logical Link Control

M&S	Modeling & Simulation
MACOM	Major Army Command
MAGTF	Marine Air Ground Task Force
MAN	Metropolitan-Area Network
Mbps	Megabits per second
MCG&I	Mapping Cartographic, Geospatial & Imaging
MDA	Milestone Decision Authority
MHS	Message Handling System
MIB	Management Information Base
MIDS	Multifunctional Information Distribution System
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
MIME	Multipurpose Internet Mail Extensions
MISSI	Multilevel Information System Security Initiative
MPEG	Motion Pictures Expert Group
MSP	Message Security Protocol

NCSC	National Computer Security Center (see NSA)
NDI	Non-developmental Item
NES	Network Encryption System
NIST	National Institute of Standards and Technology
NITF	National Imagery Transmission Format
NITFS	NITF Standard
NLSP	Network Layer Security Protocol
NNTP	Network News Transfer Protocol
NSA	National Security Agency
NSTISS	National Security Telecommunications and Information Systems

OA	Operational Architecture
ODBC	Open Data Base Connectivity
ODISC4	Office of the Director of Information Systems for Command, Control, Communications, and Computers
ODMG	Object Data Management Group
OMB	Office of Management and Budget
OOT	Object Oriented Technology
ORD	Operational Requirements Document
OSA	Open Systems Architecture
OSE	Open Systems Environment
OSF	Open Software Foundation
OSI	Open Systems Interconnection
OS-JTF	Open Systems- Joint Task Force
OSPF	Open Shortest Path First
P3I	Pre-Planned Product Improvements
PC	Personal Computer
PCAT	PC-Access Tool
PCMCIA	Personal Computer Memory Card International Association
PDU	Protocol Data Unit
PEO	Program Executive Office
PHIGS	Programmers Hierarchical Interactive Graphics System
PM	Program/Product Manager
PNNI	Private Network-Network Interface
POSIX	Portable Operating System Interface
PPP	Point-to-Point Protocol
PPS	Precise Position Service
PRI	Primary Rate Interface
PSM	Persistent Stored Modules
PTTI	Precise Time and Time Interval
RADIUS	Remote Authentication Dial In User Service
RDT&E	Research, Development, Test & Evaluation
RFC	Request for Comment
RFP	Request for Proposal
RPC	Remote Procedure Calls
RPF	Raster Product Format
RS	Recommended Standard

SA	Systems Architecture
SAMP	Security Association Management Protocol
SATCOM	Satellite Communications
SDBN	Selective Directed Broadcast Mode
SDE	Secure Data Exchange
SDNS	Secure Data Network System
SEA	Strategic Enterprise Architecture
SGML	Standard Generalized Markup Language
SHA	Secure Hash Algorithm
S-HTTP	Secure HyperText Transfer Protocol
SILS	Standard for Interoperable LAN Security
SMI	Structure of Management Information
SMIB	Security Management Information Base
SMT	Station Management
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer (of HTTP)
STD	Standard
SUS	Single UNIX Specification
TA	Technical Architecture
TACO2	Tactical Communications Protocol 2
TNS	Tactical Name Service
TADIL	Tactical Digital Information Link
TAFIM	Technical Architecture Framework for Information Management
TBM	Theater Battle Management
TCP	Transmission Control Protocol
TCSEC	Trusted Computer Security Evaluation Criteria
TEED	Tactical End-to-End Encryption Device
TELNET	Telecommunications Network
TIDP	Technical Interface Design Plan
TLSP	Transport Layer Security Protocol
TMG	Tactical Multinet Gateways
TRM	Technical Reference Model
UAV	Unmanned Aerial Vehicle
UCS	Universal Multiple-Octet Coded Character Set
UDP	User Datagram Protocol
UFD	User Functional Description
UHF	Ultra High Frequency
UPE	User Portability Extensions
URL	Uniform Resource Locator

USMC	United States Marine Corps
USMTF	United States Message Text Format
V	Version
VITD	Vector Interim Terrain Data
VMF	Variable Message Format
VPF	Vector Product Format
VTC	Video Teleconferencing
WAN	Wide Area Network
WS	Weapon System
WSTAWG	Weapon System Technical Architecture Working Group
WVS	World Vector Shoreline
WWMCCS	World-Wide Military Command and Control System
WWSS	Warfare and Warfare Support System
WWW	World Wide Web
XFN	X/Open Federated Naming

APPENDIX B - LIST OF REFERENCES

B.1 MILITARY

B.1.1 DOD References

DDS-2600-5502-87, Security Requirements for System High and Compartmented Mode Workstations, Defense Intelligence Agency, November 1987 (This document contains the same information as MITRE Technical report 9992, Revision 1)

DDS-2600-5984-01, DOD Intelligence Information Systems (DODIIS) Network Security for Information Exchange (DNSIX), (Defense Intelligence Agency (DIA)

DDS-2600-5984-91, DNSIX Interface Specifications, Version 2.1 (Final), Defense Intelligence Agency, October 1991 (This document contains the same information as MITRE Technical report 10684, Revision 1)

DDS-2600-5985-91, DNSIX Detailed Design Specifications, Version 2.1 (Final), Defense Intelligence Agency, October 1991 (This document contains the same information as MITRE Technical report 10704, Revision 1)

DDS-2600-6215-91, Compartmented Mode Workstation Labeling: Source Code and User Interface Guidelines, Defense Intelligence Agency, 1991 (This document contains the same information as MITRE Technical report 10648, Revision 1)

DDS-2600-6216-91, Compartmented Mode Workstation Labeling: Encodings Format, Defense Intelligence Agency, 1991 (This document contains the same information as MITRE Technical report 10649)

DDS-2600-6243-91 1991, Compartmented Mode Workstation Evaluation Criteria, Version 1 (Final), Defense Intelligence Agency, November 1991

DII 10164-9, SC21 N9390, Information Technology - Open System Interconnection - Systems Management - Part 9: Objects and Attributes for Access Control (final text)

DOD 3405.1, Computer Programming Language Policy, 2 April 1987

DOD 5200.1-R, Information Security Program Regulation, August 1982

DOD 5200.28-STD, DOD Trusted Computer System Evaluation Criteria

DOD 5220.22-M, Industrial Security Manual for Safeguarding Classified Information, January 1991

DOD 5220.22-R, Industrial Security Regulation, December 1985

DOD 5200.28-STD, DOD Trusted Computer System Evaluation Criteria (Orange Book), December 1985

DOD 8320.1-M, Department of Defense Data Administration Procedures, March 1994

DOD 8320.1-M-1, Department of Defense Data Element Standardization Procedures, January 1993

DOD 8320.1-M-X, Department of Defense Enterprise Data Model Development Approval and Maintenance Procedures, November 1994

DOD Directive 5200.28, Security Requirements for Automated Information Systems, 21 March 1988

ICD-GPS-060, Precise Time and Time Interval (PTTI) Interface, Rev A

ICD-GPS-153, GPS User Equipment Radio Receivers (Draft)

ICD-GPS-155, GPS Receiver Application Module Interface, Parallel Dual Port Interface (Draft)

Joint Pub 6-04, US Message Text Format (USMTF) Program, 1 October 1992

Joint Pub 6-01.5, JTIDS Technical Interface Design Plan TIDP) Test Edition, Reissue 3, Volumes 1-5, August 1994

MIL-D 89020, Digital Terrain Elevation Data (DTED)

MIL-HDBK 1300A, National Imagery Transmission Format Standard (NITFS)

MIL-PRF-28000A, Initial Graphics Exchange Specification (IGES)

MIL-STD-188-114A, Electrical Characteristics of Digital Interface Circuits

MIL-STD-188-176 (Draft)

MIL-STD-188-200, System Design And Engineering Standards For Tactical Communications

MIL-STD-188-220A, Interoperability Standard for Digital Message Transfer Device Subsystem

MIL-STD-2045-13500-2, Information Technology - DOD Profiles - Internet Relay Profile For DOD Communications

MIL-STD-2045-13502, Information Technology Defense Standardized Profiles, Dynamic Internet Routing Between Autonomous Systems

MIL-STD-2045-14502-1A, Information Technology Internet Transport Profile For DOD Comm.: Transport & Internet Services

MIL-STD-2045-14502-2, Information Technology Internet Transport Profile For DOD Comm.: Transport & Internet Services

MIL-STD-2045-14502-3, Information Technology Internet Transport Profile For DOD Comm.: Transport & Internet Services

MIL-STD-2045-14502-4/5, Information Technology Internet Transport Profile For DOD Comm.

MIL-STD-2045-14502-6A, Information Technology Internet Transport Profile For DOD Comm.

MIL-STD-2045-14503, Information Technology - DOD Profiles - Internet Transport Service Supporting OSI Applications

MIL-STD-2045-17501, Message Handling System (MHS) Common Messaging

MIL-STD-2045-17502, Message Handling System (MHS) Military Messaging (P772)

MIL-STD-2045-17505, Info. Tech. DOD Standardized Profile Internet Domain Name System (DNS)

MIL-STD-2045-18500, Message Handling System (MHS) Message Security Protocol

MIL-STD-2045-17504, Internet File Transfer Profile

MIL-STD-2045-17506, Internet Remote Login Profile

MIL-STD-2045-17507, Simple Network Management Protocol (SNMP) Profile

MIL-STD-2045-47001, Interoperability Standard For Connectionless Data Transfer Application Layer Standard

MIL-STD 2407, Vector Product Format (VPF) - DMA format for vector-based products, such as Vector Map (Vmap), Digital Nautical Chart (DNC), Vector Interim Terrain Data (VITD), and World Vector Shoreline (WVS)

MIL-STD 2411, Raster Product Format (RPF) - Defense Mapping Agency (DMA) format for raster-based products, such as Compressed ARC Digitized Raster Graphics (CADRG) and Controlled Image Base (CIB).

MIL-STD-2500, National Imagery Transmission Format (NITF), Version 2.0

MIL-STD-2525, Common Warfighting Symbology, Version 1, 30 September 1994

MIL-STD-6040, US Message Text Format (USMTF) Electronic Document System, CDU95V01, 1 October 1995 (formerly Joint Pub 6-04)

NCSC-TG-021, Version-1, Trusted Database Management System Interpretation, April 1991

ODMG-93

(No Number) ASD Memorandum Development, Procurement, and Employment of DoD Global Position System User Equipment, 31 April 1992

(No Number) ASD (C3I) memorandum, 31 October 1994

(No Number) Defense Information Systems Security Program (DISSP) Goal Security Architecture (DGSA), Defense Information Systems Agency (DISA), Arlington VA, 30 June 1993 (Draft)

(No Number) Department of Defense (DOD). 1994b. *Department of Defense Human Computer Interface Style Guide* (Version 2.0), Defense Information Systems Agency Center for Information Management, McLean, VA

(No Number) DII COE Integration and Runtime Specification (I&RTS), Version 2.0, October 1995

(No Number) DOD Memorandum, Subject: Accelerated Implementation of Migration Systems, Data Standards, and Process Improvement, 13 October 1993

(No Number) DOD Memorandum, Subject: Specifications & Standards -- A New Way of Doing Business, 29 June 1994

(No Number) DOD Technical Architecture Framework for Information Management (TAFIM), 30 June 1994. Volume 8 of this document is the DOD HCI Style Guide

(No Number) DODIIS Client Server Environment Specifications (Draft), DODIIS Management Board, Washington DC, 1992

(No Number) DODIIS Profile of the DOD Technical Reference Model for Information Management (Draft), DODIIS Management Board, Washington DC, June 1993

(No Number) DODIIS Reference Model for the 1990s, DODIIS Management Board, Washington DC, December 1992

(No Number) FORTEZZA Cryptologic Interface Programmers Guide for the Fortezza Crypto Card, Version 1.51, 15 May 1995

(No Number) FORTEZZA Interface Control Document, Revision P1.5, 22 December 1994, FOUO

(No Number) FORTEZZA Plus Interface Control Document, Release 3.0, 1 June 1995, FOUO

(No Number) GCCS COE 2.0 Baseline Document, 6 March 1995

(No Number) Interface Control Document for the FORTEZZA Crypto Card, Version P1.5, 22 December 1994

(No Number) Joint VMF TIDP

(No Number) JTIDS TIDP Test Edition

(No Number) User Interface Specification for the Defense Information Infrastructure(DII) Version 1.0 (Draft)

(No Number) User Interface Specifications for the Global Command and Control System (GCCS), October 1994

(No Number) User Interface Specifications for the GCCS

B.1.2 Army References

ACCS-A3-407-008C, Interface Specification for the Army Data Distribution System (ADDS) Interface, 8 March 1991

ACCS-A3-407-008D, Interface Specification for the Army Data Distribution System (ADDS) Interface

AR 380-19, Army Regulation, Information Systems Security, 1 August 1990

MIL-STD-188-220A, Interoperability Standard for Digital Message Transfer Device Subsystems, 28 February 1995

(No Number) Command and Control (C2) Core Data Model, Version 2, Defense Information Systems Agency, 1 July 1994

(No Number) DOD Enterprise Model, A White Paper, Office of the Director of Defense Information, Office of the Secretary of Defense, February 1993

(No Number) HQDA Memorandum, Subject: 1994 Army Science Board Study: Technical Architecture for Army C4I, 28 July 1994

(No Number) Task Force XXI VMF Technical Interface Design Plan (TIDP)

(No Number) The Army Enterprise Implementation Plan, 8 August 1994

(No Number) The Army Enterprise Strategy, the Vision, 20 July 1993

(No Number) Variable Message Format Technical Interface Design Plan for Task Force XXI, 30 November 1994

B.1.3 Other Government Agency References

FIPS Pub JJJ, Standard for Public Key Authentication

FIPS Pub 46-2, Data Encryption Standard, December 1993

FIPS Pub 120-1 (change notice 1), Graphical Kernel System (GKS)

FIPS Pub 127-2, Database Language - SQL

FIPS Pub 128, Computer Graphics Metafile (CGM)

FIPS Pub 152, Standard Generalized Markup Language (SGML)

FIPS Pub 153, Programmers Hierarchical Interactive Graphics Systems (PHIGS)

FIPS Pub 158-1 Federal Information Processing Standards Publication 158-1, The User Interface Component of the Applications Portability Profile (X Window System, Version 11, Release 5), 8 October 1993

FIPS Pub 161-1, Electronic Data Interchange (EDI)

FIPS Pub 180, National Institute of Standards and Technology (NIST) Secure Hash Algorithm (SHA), 11 May 1993

FIPS Pub 183, Federal Information Processing Standards Publication 183, Integration Definition for Function Modeling (IDEF0), 21 December 1993

FIPS Pub 184, Federal Information Processing Standards Publication 184, Integration Definition for Data Modeling (IDEF1X), 21 December 1993

FIPS Pub 185, NIST Escrowed Encryption Standard, 9 February 1994

FIPS Pub 186, NIST Digital Signature Standard (DSS) algorithm, 19 May 1994

LL-500-04-03,GCCS Common Operating Environment Baseline, 28 November 1994

NCSC-TG-005, National Computer Security Center, Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria (Red Book), 31 July 1987

NISTIT 90-4250

NSTISS No. 4009, National Security Telecommunications and Information Systems Security, National Information System Security (INFOSEC) Glossary, 5 June 1992

OMB Circular A-71, Office of Management of the Budget, Transmittal Memorandum No. 1, Security of Federal Automated Information Systems, 27 July 1978

OMB Circular A-123, Internal Control Systems, 5 November 1981

(No Number) GCCS Integration Standard, Version 1, 26 October 1994

(No Number) NSA-developed Type II Confidentiality Algorithm (SKIPJACK)

(No Number) NSA-developed Type II Key Exchange Algorithm (KEA)

(No Number) User Interface Specifications for the Global Command and Control Systems (GCCS), Version 1, October 1994

B.2 COMMERCIAL REFERENCES

ACP 123, Allied Communication Publication

AMHS 1, (U.S. Supplement to ACP 123)

ANSI X3.229, Fiber Distribution Data Interface (FDDI) - Station Management (SMT)

CCITT X.25, CCITT Recommendation X.25: "Interface Between Data Terminal Equipment (DTE) and Data Circuit Terminating Equipment (DCE) for Terminals Operating in the Packet Mode on Public Data Networks," International Telegraph and Telephone Consultative Committee

CSC-STD-004-85, Technical Rationale Behind CSCSTD00385: Computer Security Requirements, National Computer Security Center, 25 June 1985

DIS 9075-4, Database Language SQL, Part 4: Persistent Stored Modules (SQL/PSM) (Draft)

ESD-TR-86-278, *Guidelines for Designing User Interface Software* (Smith and Mosier 1986)

I.430

I.431

IDUP-GSS-API, Independent Data Unit Protection Generic Security Service Application Program Interface, 7 June 1995

IEEE 802.2, Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements--Part 2: Logical link control, 1994

IEEE 802.3, Information technology--Local and metropolitan area networks--Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications, 1993

IEEE 802.3u, Information technology--Local and metropolitan area networks--Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications, 1995

IEEE 802.10, IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS), IEEE, 1992

IEEE 802.10a, Standard for Interoperable LAN Security-The Model, IEEE, Draft Jan 1989

IEEE 802.10b, Standard for Interoperable LAN Security-Part B: Secure Data Exchange, 1992

IEEE 802.10c/D6, Standard for Interoperable LAN Security-Part C: Key Management, Draft 6 issued 1994

IEEE 802.10d, Standard for Interoperable LAN Security-Part D: Security Management, (Draft)

IEEE 1003.1, POSIX: System API (with FIPS Pub 151-2 profile), POSIX: Portable Operating System Interface for Computer Environments

IEEE 1003.1c, POSIX: System API - Threads and Extensions

IEEE 1003.1i, POSIX: System API - Real-time Extensions

IEEE 1003.2, POSIX: Shell and Utilities (with FIPS Pub 189-1 profile)

IEEE 1003.2d, POSIX: Shell and Utilities - Batch Environment

IEEE 1003.5:1992, POSIX: Ada Language Interfaces Part 1: Binding for System API

IEEE 1003.5b, POSIX (Draft)

IEEE 1003.6, POSIX Security Enhancements

IEEE 1278.1, DIS Application Protocols, 1995

IEEE 1278.2, DIS Communication Services and Profiles, 1995

IEEE 1278.3, DIS Exercise Management and Feedback, 1995

IETF RFC 822, Version 3.0 Hyper Text Mark-up Language (HTML)

ISO 7498, Information Processing Systems - Open Systems Interconnection - Basic Reference Model

ISO 7498-2, Security Service Recommendations, 1989

ISO 7776, Information Processing Systems - Data Communication High-Level Data Link Control Procedures - Description of the X.25 LAPB-compatible DTE Data Link Procedures, 1986

ISO 8208, Information Processing Systems - Data Communications - X.25 Packet Layer Protocol for Data Terminating Equipment, 1989

ISO 8652, Ada Reference Manual, Language and Standard Libraries, 15 February 1995

ISO 9314-1, Info Proc Sys - Fibre Distributed Data Interface (FDDI) - Pt 1: Token Ring Physical Layer Protocol (PHY)

ISO 9314-2, Info Proc Sys - Fibre Distributed Data Interface (FDDI) - Pt 2: Token Ring Media Access Control (MAC)

ISO 9314-3, Info Proc Sys - Fibre Distributed Data Interface (FDDI) - Pt 3: Physical Layer Medium Dependent (PMD)

ISO 10181, OSI Security Frameworks

ISO 10918-1, Joint Picture Expert Group (JPEG)

ISO 11172, Information Technology - Coding of Moving Pictures and Associated Audio for Digital Storage Media up to 1.5 Mbps

ISO 12227:1994, SQL Ada Module Description Language

ISO 13818, Motion Picture Experts Group (MPEG-2)

ISO/IEC 8859-1:1987, Information Processing - 8-Bit Single-Byte Coded Character Sets

ISO/IEC 9075-3: 1995, Call Level Interface (Draft)

ISO/IEC 9596-1, 1991, Information Technology - Open Systems Interconnection - Common Management Information Protocol (CMIP) - Part 1: Specification

ISO/IEC 9636, Information Technology-Computer Graphics-Interfacing Techniques for Dialogue with Graphics Devices (CGI)

ISO/IEC 9798-1, 1991 Entity Authentication Mechanisms, Part 1- 4: General Model

ISO/IEC 10021-1 1990/DAM 4, Information Technology-Message Handling Systems (MHS)

ISO/IEC 10164-7, 1992, Information Technology-Open System Interconnection - Systems Management - Part 7: Security Alarm Reporting Function, ISO/IEC JTC1 SC21/WG4, IS May 1992

ISO/IEC 10165, Series, Information Technology - Open Systems Interconnection - Structure of Management Information - Parts 1- 4, 1993 - 1994

ISO/IEC 10646-1:1993, Information Technology - Universal Multiple-Octet Coded Character Set (UCS)

ISO/IEC 10736, 199X, SC6 N8455, Information Technology-Open Systems Interconnection-Transport Layer Security Protocol Plus Amendment 1 on Security Association Establishment Protocol

ISO/IEC 11577, 199X, SC6 N8453, Information Technology-Telecommunications and Information Exchange Between Systems

ISO/IEC DII 10181, Series, Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems, 1994 - 1995

ISP-421/94.05.15 Revision 1.0, The ISDN Security Program (ISP) Security Association Management Protocol (SAMP)

ITU H.320, Line Transmission Of Non-Telephone Signals Narrow-Band Visual Telephone Systems And Terminal Equipment

ITU H.321

ITU H.323

ITU H.324

ITU-T Rec. X.500, Directory Infrastructure

ITU-T Rec. X.509, version 3, Directory Authentication Framework

ITU-T X.274

ITU-T X.711, 1991

ITU-T X.736, 1992

ITU X.25, Interface Between DTE & DCE For Trmnls Oper. In The Packet Mode & Conn. To Public Data Ntwrks By Dedicated Circ.

ODBC 2.0, Open Data Base Connectivity,

OSF 1992, Open Software Foundation (OSF)/MotifTM Style Guide, Revision 1.2

P315, DCE Authentication and Security Specification (Draft)

Q.921

Q.931

RFC-904, Mills, D., Exterior Gateway Protocol Formal Specification, April 1984

RFC-951, Croft, W.; Gilmore, J., Bootstrap Protocol, September 1985

RFC-1075, S. Deering, C. Partridge, D. Waitzman, Distance Vector Multicast Routing Protocol, November 1988

RFC-1356, Malis, A.; Robinson, D.; Ullmann, R., Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode, August 1992

RFC-1441, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, Introduction to version 2 of the Internet-standard Network Management Framework, May 1993

RFC-1442, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2), May 1993

RFC-1443, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, Textual Conventions for version 2 of the Simple Network Management Protocol (SNMPv2), May 1993.

RFC-1444, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, Conformance Statements for version 2 of the Simple Network Management Protocol (SNMPv2), May 1993

RFC-1445, J. Davin, K. McCloghie, Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2), May 1993.

RFC-1446, J. Galvin, K. McCloghrie, Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2), May 1993

RFC-1447, K. McCloghrie, J. Galvin, Party MIB for version 2 of the Simple Network Management Protocol (SNMPv2), May 1993

RFC-1448, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2), May 1993

RFC-1449, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, Transport Mappings for version 2 of the Simple Network Management Protocol (SNMPv2), May 1993

RFC-1450, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, Management Information Base for version 2 of the Simple Network Management Protocol (SNMPv2), May 1993

RFC-1451, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, Manager to Manager Management Information Base, May 1993

RFC-1452, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, Coexistence between version 1 and version 2 of the Internet-standard Network Management Framework, May 1993

RFC 1508, Generic Security Service Application Program Interface (GSS-API), September 1993

RFC-1531, Droms, R. Dynamic Host Configuration Protocol, October 1993

RFC-1533, Alexander, S.; Droms, R. DHCP Options and BOOTP Vendor Extensions, October 1993

RFC-1534, Droms, R. Interoperation Between DHCP and BOOTP, October 1993

RFC-1541, R. Droms, Dynamic Host Configuration Protocol, October 1993

RFC-1542, Wimer, W. Clarifications and Extensions for the Bootstrap Protocol, October 1993

RFC-1577, M. Laubach, Classical IP and ARP over ATM, January 1994

RFC-1583, Moy, J. OSPF Version 2, March 1994

RFC-1584, J. Moy, Multicast Extensions to OSPF, March 1994

RFC-1618, W. Simpson, PPP over ISDN, May 1994

RFC-1654, Rekhter, Y.; Li T. A Border Gateway Protocol 4 (BGP-4), July 1994

RFC-1661, Simpson, W. The Point-to-Point Protocol (PPP), July 1994

RFC-1738, T. Berners-Lee, L. Masinter, M. McCahill, Uniform Resource Locators (URL), December 1994

RFC-1770, Graff C.; IPv4 Option for Sender Directed Multi-Destination, March 1995

RFC-1808, R. Fielding, Relative Uniform Resource Locators, July 1995

RFC 1825, Security Architecture for the Internet Protocol, August 1995

RFC 1826, IP Authentication Header, August 1995

RFC 1827, IP Encapsulating Security Payload (ESP), August 1995

RFC 1828, IP Authentication using Keyed MD5, August 1995

RFC 1829, The ESP DES-CBC Transform, August 1995

RS-232-D, EIA Standard, Interface Between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange, June 1981

RS-449, EIA Standard, General Purpose 37-Position and 9-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange, November 1987

RS-530, High-Speed 25-Position Interface for Data Terminal Equipment and Data-Circuit Terminating Equipment

STD-3, Host Requirements, R. Braden, October 1989 (Also RFC-1122, RFC-1123)

STD-4, Gateway Requirements, R. Braden, J. Postel, June 1987 (Also RFC-1009)

STD-5, Internet Protocol, J. Postel, September 1981 (Also RFC-791, RFC-950, RFC-919, RFC-922, RFC-792, RFC-1112)

STD-6, User Datagram Protocol, J. Postel, August 1980 (Also RFC-768)

STD-7, Transmission Control Protocol, J. Postel, September 1981 (Also RFC-793)

STD-8, Telnet Protocol, J. Postel, J. Reynolds, May 1983 (Also RFC-854, RFC-855)

STD-9, File Transfer Protocol, J. Postel, J. Reynolds, October 1985.(Also RFC-959)

STD-13, Domain Name System, P. Mockapetris, November 1987 (Also RFC1034, RFC1035)

STD-15, Simple Network Management Protocol, J. Case, M. Fedor, M. Schoffstall, J. Davin, May 1990 (Also RFC-1157)

STD-16, Structure of Management Information, M. Rose, K. McCloghrie, May 1990 (Also RFC-1155, RFC-1212)

STD-17, Management Information Base, K. McCloghrie, M. Rose, March 1991. (Also RFC-1213)

STD-35, ISO Transport Service on top of the TCP (Version: 3), M. Rose, D. Cass, May 1978 (Also RFC-1006)

STD-36, Transmission of IP and ARP over FDDI Networks, D. Katz, January 1993 (Also RFC-1390)

STD-41, Standard for the Transmission of IP Datagrams over Ethernet Networks, C. Hornig, April 1984 (Also RFC-894)

STD-43, Standard for the Transmission of IP Datagrams over IEEE 802 Networks, J. Postel, J.K. Reynolds, August 1993 (Also RFC-1042)

STD-51, PPP in HDLC-like Framing, W. Simpson, Editor, July 1994 (Obsoletes RFC1549) (Also RFC1662)

WD 9798-5, SC27 N 1104 (Project 1.27.03.05), Entity Authentication Mechanisms - Part 5

X/Open C309, DCE Remote Procedure Call

X/Open C310, DCE Time Services

X/Open C312, DCE Directory Services

X/Open C403, DCE: X/Open Federated Naming (XFN) Specification

(no number) ATM Forum's User-Network Interface Specification, Version 3.1

(no number) Common Object Request Broker Architecture (CORBA) 2.0 (Draft)

(no number) Common Open Software Environment (COSE) Common Desktop Environment (CDE) (Draft)

(no number) FTP Security Extensions, M. Horowitz, S. Lunt, 7 July 1995 (Draft)

(no number) GSS-API Authentication Method for SOCKS Version 5, 5 July 1995 (Draft)

(no number) IGOSS The Industry/Government Open Systems Specification, Draft, January 1993

(no number) Industry Video Teleconferencing Profile, the Corporation for Open Systems (COS)

(no number) Internet Draft July 95 - Jan 96

(no number) Internet Draft June 95 - Dec 95, Version 3

(no number) Open Software Foundation (OSF)/MotifTM Style Guide, Revision 1.2 (OSF 1992)

(no number) OSF/Motif Inter Client Communications Convention Manual (ICCCM)

(no number) Remote Authentication Dial In User Service (RADIUS), et. al., May 1995 (Draft)

(no number) SOCKS Protocol Version 5, 4 October 1995 (Draft)

(no number) The WindowsTM Interface: An Application Design Guide, Microsoft Press, 1992

(no number) Username/Password Authentication for SOCKS V5, 30 May 1995 (Draft)

(no number) Win32 APIs, Microsoft Win32 Programmers Reference Manual, Volumes 5, Microsoft Press, January 1993

(no number) Win32 APIs, Window Management and Graphics Device Interface, Volume 1, Microsoft Win32 Programmers Reference Manual, Microsoft Press, 1993

(no number) X/Open Single UNIX Specification (SUS)

(no number) 25.6 Mb/s over Twisted Pair Cable Physical Interface, ATM Forum UNI 3.1

This page was intentionally left blank.

APPENDIX C - GLOSSARY

Access control

Process of limiting access to the resources of an IT product only to authorized users, programs, processes, systems, or other IT products.

Accreditation

The managerial authorization and approval, granted to an ADP system or network to process sensitive data in an operational environment, made on the basis of a certification by designated technical personnel of the extent to which design and implementation of the system meet pre-specified technical requirements, e.g., TCSEC, for achieving adequate data security. Management can accredit a system to operate at a higher/lower level than the risk level recommended (e.g., by the Requirements Guidelines) for the certification level of the system. If management accredits the system to operate at a higher level than is appropriate for the certification level, management is accepting the additional risk incurred.

Application Platform Entity

The application platform is defined as the set of resources that support the services on which application software will execute. It provides services at its interfaces that, as much as possible, make the implementation-specific characteristics of the platform transparent to the application software. (TAFIM, Version 2.0, Volume 2)

Applications Portability

The ability to move an application from one support environment to a different support environment, such that there is no change in the application's functional operation. A support environment is the set of hardware and software resources required by an application to perform its functions.

Application Software Entity

Mission-area and support applications. A common set of support applications forms the basis for the development of mission-area applications. Mission-area should be designed and developed to access this set of common support applications. Applications access the Application Platform via a standard set of APIs. (TAFIM, Version 2.0, Volume 2)

Architecture

An architecture is a composition of (1) components (including humans) with their functionality defined (Technical), (2) requirements that have been configured to achieve a prescribed purpose or mission (Operational), and (3) their connectivity with the information flow defined (System). (OS-JTF)

Authentication

(1) To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

(2) To verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification.

Character-based interface

A non-bit mapped user interface in which the primary form of interaction between the user and system is through text.

Commercial Item

1) Any item customarily used by the general public for other than governmental purposes, that has been sold, leased, or licensed to the general public, or that has been offered for sale, lease or license to the general public.

2) Any item that evolved from an item described in 1) above through advances in technology or performance that is not yet available in the commercial market, but will be available in time to meet the delivery requirements of the solicitation.

3) Any item that, but for modifications of a type customarily available in the commercial market or minor modifications made to meet DOD requirements, would satisfy the criteria in 1) or 2) above.

4) Any combination of items meeting the requirements of 1, 2, or 3 above or 5 below that are of a type customarily combined and sold in combination to the general public.

5) Installation services, maintenance services, repair services, training services, and other services if such services are procured for support of any item referred to paragraphs 1, 2, 3. or 4 above, if the sources of such services

- offers such services to the general public and the DOD simultaneously and under similar terms and conditions and
- offers to use the same work force for providing the DOD with such services as the source used for providing such services to the general public.

6) Services offered and sold competitively, in substantial quantities, in the commercial marketplace based on established catalog prices of specific tasks performed and under standard commercial terms and conditions.

7) Any item, combination of items or service referred to in 1 through 6 above notwithstanding the fact that the item or service is transferred between or among separate divisions, subsidiaries, or affiliates of a contractor.

8) A nondevelopmental item developed exclusively at private expense and sold in substantial quantities, on a competitive basis, to State and local governments.

(DRAFT 6/30/95 NDI HANDBOOK/ Federal Acquisition Streamlining Act of 1994 DOD 5000.37H)

Commercial-off-the-shelf (COTS)

See the definition of Commercial Item found above. (OS-JTF 1995)

Compliance

Compliance is enumerated in an implementation/migration plan. A system is compliant with the ATA if it meets, or is implementing an approved plan to meet, all applicable ATA mandates.

Data Integrity

(1) The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction.

(2) The property that data has not been exposed to accidental or malicious alteration or destruction.

Domain

A distinct functional area that can be supported by a family of systems with similar requirements and capabilities. An area of common operational and functional requirements.

Graphical User Interface (GUI)

System design that allows the user to effect commands, enter into transaction sequences, and receive displayed information through graphical representations of objects (menus, screens, buttons, etc.).

Human-Computer Interface (HCI)

Hardware and software allowing information exchange between the user and the computer.

Hybrid Graphical User Interface

A GUI that is composed of toolkit components from more than one user interface style.

Integration

Two or more software applications that must run on the same physical processor(s) and under the same operating system.

Interoperability

(1) The ability of two or more systems or components to exchange data and use information. (IEEE STD 610.12)

(2) The ability of two or more systems to exchange information and to mutually use the information that has been exchanged. (Army Science Board)

Intraoperability

Interoperability within a designated domain or boundary. (OS-JTF)

Market Acceptance

Means that an item has been accepted in the market as evidenced by annual sales, length of time available for sale, and after-sale support capability. (DRAFT 6/30/95 NDI HANDBOOK/ Federal Acquisition Streamlining Act of 1994 DOD 5000.37H)

Motif

User interface design approach based upon the "look and feel" presented in the OSF/MotifTM style guide. MotifTM is marketed by the Open Software Foundation.

Non Developmental Item (NDI)

1) Any commercial item.

2) Any previously developed item in use by a US Federal, State or Local government agency or a foreign government with which the US has a mutual defense cooperation agreement.

3) Any item described in subparagraph 1 or 2, above, that requires only minor modification in order to meet the requirements of the procuring agency.

4) Any item currently being produced that does not meet the requirement of paragraphs 1, 2, or 3 above, solely because the item is not yet in use.

(DRAFT 6/30/95 NDI HANDBOOK/ Federal Acquisition Streamlining Act of 1994 DOD 5000.37H)

Open Software Foundation (OSF)

Consortium of computer hardware and software manufacturers whose membership includes over seventy of the computer industry's leading companies.

Open System

A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered components to be utilized across a wide range of systems with minimal changes, to interoperate with other components on local and remote systems, and to interact with users in a style that facilitates portability. An open system is characterized by the following:

- Well defined, widely used, non-proprietary interfaces/protocols, and

- Use of standards which are developed/adopted by industrially recognized standards bodies, and

-Definition of all aspects of system interfaces to facilitate new or additional systems capabilities for a wide range of applications, and

- Explicit provision for expansion or upgrading through the incorporation of additional or higher performance elements with minimal impact on the system.

(IEEE POSIX 1003.0/D15 as modified by the Tri-Service Open Systems Architecture Working Group)

Open Systems Approach

An open systems approach is a business approach that emphasizes commercially supported practices, products, specifications and standards. The approach defines, documents, and maintains a system technical architecture that depicts the lowest level of system configuration control. This architecture clearly identifies all the performance characteristics of the system including those that will be accomplished with an implementation that references open standards and specifications. (OS-JTF)

Open Systems Architecture (OSA)

A system architecture produced by an open systems approach and employing open systems specifications and standards to an appropriate level. (OS-JTF)

Operational Architecture (OA)

An **Operational Architecture** is a description, often graphical, which defines the force elements and the requirement to exchange information between these force elements. It defines the types of information, the frequency of its exchange, and what warfighting tasks are supported by these information exchanges. It specifies what the information systems are operationally required to do and where these operations are to be performed. (C4I Service Chiefs Warrior Focused Definitions, Jan 96)

Portability

The ease with which a system, component, data, or user can be transferred from one hardware or software environment to another. (TAFIM, Version 2.0, Volume 1/3)

Real Time

Real time is a mode of operation. Real Time systems require events, data, and information to be available in time for the system to perform its required course of action. Real Time operation is characterized by scheduled event, data, and information meeting their acceptable arrival times. (OS-JTF)

Real Time Systems

Systems which provide a deterministic response to asynchronous inputs. (OS-JTF)

Reference Model

A reference model is a generally accepted abstract representation that allows users to focus on establishing definitions, building common understandings and identifying issues for resolution. For Warfare and Warfare Support System (WWSS) acquisitions, a reference model is necessary to establish a context for understanding how the disparate technologies and standards required to implement WWSS relate to each other. Reference modules provide a mechanism for identifying key issues associated with portability, scalability, and interoperability. Most importantly reference modules will aid in the evaluation and analysis of domain specific architectures. (TRI-SERVICE Open Systems Architecture Working Group)

Scalability

The capability to adapt hardware or software to accommodate changing work loads. (OS-JTF)

Security

(1) The combination of confidentiality, integrity, and availability.

(2) The quality or state of being protected from uncontrolled losses or effects. Note: Absolute security may in practice be impossible to reach; thus the security "quality" could be relative. Within state models of security systems, security is a specific "state" that is to be preserved under various operations.

Single user Computer

A computer that is operated by one user at a time. A user is an entity such as a human, sensor, or software process that interacts with the computer.

Standard

A document that establishes uniform engineering and technical requirements for processes, procedures, practices, and methods. Standards may also establish requirements for selection, application, and design criteria of material. (DOD 4120.3-M)

Standards based architecture

Is an architecture based on an acceptable set of standards governing the arrangement, interaction, and interdependence of the parts or elements that together may be used to form a weapons systems, and whose purpose is to insure that a conformant system satisfies a specified set of requirements. (OS-JTF)

System

(1) People, machines and methods organized to accomplish a set of specific functions. (FIPS 11-3)

(2) An integrated composite of people, products, and processes that provides a capability or satisfy a stated need or objective. (DOD 5000.2)

(3) In the ATA, the term "system" refers to those items that produce, use or exchange information.

(4) Systems of systems such as ASAS or AFATDS are NOT considered monolithic systems for ATA compliance. For example, targeting and fire direction data passed to the fire direction center may come from outside the local system and travel over common data networks, and therefore compliance with the ATA is an important design consideration.

Systems Architecture (SA)

A **Systems Architecture** is a description, often graphical, of the systems solution used to satisfy the warfighter's Operational Architecture requirement. It defines the physical connection, location, and identification of nodes, radios, terminals, etc. associated with information exchange. It also specifies the system performance parameters. The Systems Architecture is constructed to satisfy Operational Architecture requirements per the standards defined in the Technical Architecture. (C4I Service Chiefs Warrior Focused Definitions, Jan 96)

Technical Architecture (TA)

A **Technical Architecture** is the minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements that together may be used to form an information system. Its purpose is to ensure that a conformant system satisfies a specified set of requirements. It is the building code for the Systems Architecture being constructed to satisfy Operational Architecture requirements. (C4I Service Chiefs Warrior Focused Definitions, Jan 96)

Technical Reference Model (TRM)

A target framework and profile of standards for the DOD computing and communications infrastructure. (TAFIM, Version 2.0, Vol. 1/OS-JTF)

Weapons System

A combination of one or more weapons with all related equipment, materials, services, personnel and means of delivery and deployment (if applicable) required for self sufficiency. (JCS Pub 1-02)

This page was intentionally left blank.

APPENDIX D - SUSTAINING BASE/OFFICE AUTOMATION DOMAIN EXCEPTIONS AND EXTENSIONS

D.1 DOMAIN DESCRIPTION

The Sustaining Base/Office Automation Domain consists of automated systems that perform service support, business and office automation functions.

D.2 INFORMATION PROCESSING STANDARDS

D.2.1 Mandates

D.2.1.1 Exceptions

No exceptions to this section.

D.2.1.2 Extensions

User Interface Services

This domain shall develop or acquire applications that follow the following user interface services:

- Win32 APIs, Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers Reference Manual, 1993, Microsoft Press.

Data Management Services

This domain shall develop or acquire client applications that follow the following data management services.

- Open Data Base Connectivity, ODBC 2.0: Provides standard call level APIs between database application clients and the database server.

Operating System Services

This domain shall develop or acquire applications that follow the following operating system services:

- Win32 APIs, Microsoft Win32 Programmers Reference Manual, Volumes 1-5, 1993, Microsoft Press.

D.2.2 Emerging Standards

Within the Software Engineering Services, it is expected that publicly available Ada 95 bindings to Win32 APIs will be adopted.

D.3 INFORMATION TRANSPORT STANDARDS

There are no exceptions or extensions to this section.

D.4 INFORMATION MODELING AND DATA EXCHANGE STANDARDS

There are no exceptions or extensions to this section.

D.5 HUMAN-COMPUTER INTERFACES

D.5.1 Mandates

D.5.1.1 Exceptions

There are no exceptions to this section.

D.5.1.2 Extensions

The following commercial HCI style guide is an extension to the mandates for this domain.

- The WindowsTM Interface: An Application Design Guide, Microsoft Press, 1992.

D.5.2 Emerging Standards

There are no extensions to this section.

D.6 INFORMATION SECURITY

There are no exceptions or extensions to this section.

APPENDIX E - C3I DOMAIN EXCEPTIONS AND EXTENSIONS

E.1 DOMAIN DESCRIPTION

The C3I Domain consists of command and control, communications, intelligence, and electronic warfare systems.

E.2 INFORMATION PROCESSING STANDARDS

E.2.1 Mandates

There are no exceptions or extensions to this section.

E.2.2 Emerging Standards

Within User Interface Services, an attempt is currently being made to unify the existing Graphical User Interface standards under a common framework. One emerging commercial standard is the Common Open Software Environment (COSE) Common Desktop Environment (CDE). This framework provides not only mechanisms for graphical display of common objects, but it also provides standard interprocess communication mechanisms and a set of commonly-used desktop tools (e.g. file manager and mail tool) that are relevant to many domains.

E.3 INFORMATION TRANSPORT STANDARDS

There are no exceptions or extensions to this section.

E.4 INFORMATION MODELING AND DATA EXCHANGE STANDARDS

There are no exceptions or extensions to this section.

E.5 HUMAN-COMPUTER INTERFACES

The *User Interface Specifications for the Global Command and Control System (GCCS)* (October 1994) defines the appearance and behavior of the user interface for GCCS applications and has been adopted as the domain-level style guide for C3I systems within the Army. This document adopts X Windows and Motif and supplements the basic guidelines set forth in the *DOD HCI Style Guide.*

E.6 INFORMATION SECURITY

There are no exceptions or extensions to this section.

This page was intentionally left blank.

APPENDIX F - WEAPONS SYSTEM DOMAIN EXCEPTIONS AND EXTENSIONS

F.1 THE WEAPONS SYSTEM DOMAIN

Weapons systems communicate and receive information in support of their warfighting users. Weapons systems provide Command and Control capabilities that require gathering, processing, and communicating data to the warfighter. The systems need to be deterministic, having a real-time response to the mission critical data that requires a specific action or reaction. Weapons systems are designed to support the warfighter with the primary focus on lethality, survivability, and battle management. Weapons systems are also sensors which gather data for the larger seamless architecture, therefore they too must interact and interoperate.

The Weapon System Technical Architecture Working Group (WSTAWG) was formed in response to an ADO/DISC4 meeting that determined weapons systems should be included in the Technical Architecture effort. The WSTAWG group is comprised of representatives from the Army Program Executive Offices, Program Managers Army Research and Development Centers, and others who are engaged in building weapons systems. The WSTAWG discussed the standards - military, proprietary, and commercial, that they employ in their current system designs and briefed the results of their effort to the Army Digitization Office, Army Science Board, and Army System Engineering Office. The WSTAWG concluded that there was a need for additional domain analysis to help identify additional standards that would allow specific weapons system domains to share products, processes, and services.

The focus of the WSTAWG, for this revision of the ATA, concentrated only on interoperability standards and specifications that interface weapons systems to C4I systems and to other weapons systems. The goal remains to reduce the unit cost, life cycle cost, and deployment cost of today's weapons by incorporating Army Technical Architecture standards into designs for new and already fielded weapons systems.

Weapons systems operate in many different environments around the world. The systems include physical restrictions of size, weight, and power. Weapons systems must also meet specific performance requirements based on the mission of the platform. To this end, one standard does not fit all of the many sizes and shapes of today's Army weapons systems. As an example: operational, technical, and physical constraints associated with embedded weapons systems may not permit the use of the DII COE as currently defined. Therefore, the WSTAWG is currently exploring and identifying an extension of the DII COE for the weapons system domain. This domain specific COE implementation will allow the development of application software which can then be offered up for reuse to other systems within the weapons system domain and to other domains.

The WSTAWG is committed to its work on domain analysis to identify standards that provide a common form, fit, and function across platforms of a similar domain

(Interoperability and Intraoperability). When these standards are identified and agreed to, the WSTAWG will submit them through the Army Technical Architecture configuration management process for inclusion in the next revision.

F.2 INFORMATION PROCESSING STANDARDS

F.2.1 Mandates

F.2.1.1 Exceptions

Graphic Services

The standard that applies to this domain is:

ISO/IEC 9636, Information Technology-Computer Graphics-Interfacing Techniques for Dialogue with Graphics Devices (CGI)

F.2.2 Emerging Standards

There are no extensions to this section.

F.3 INFORMATION TRANSPORT STANDARDS

There are no exceptions or extensions to this section.

F.4 INFORMATION MODELING AND DATA EXCHANGE STANDARDS

There are no exceptions or extensions to this section.

F.5 HUMAN-COMPUTER INTERFACES

There are no exceptions or extensions to this section.

F.6 INFORMATION SECURITY

There are no exceptions or extensions to this section.

APPENDIX G - MODELING & SIMULATION DOMAIN EXCEPTIONS AND EXTENSIONS

G.1 DOMAIN DESCRIPTION

The Simulation Domain consists of those standards that support architectural efforts to combine live, virtual and constructive modeling and simulations for training and combat analysis. Distributed Interactive Simulation (DIS) is a government/industry initiative to define an infrastructure for linking simulations of various types at multiple locations to create realistic, complex, virtual "worlds" for the simulation of highly interactive activities. This infrastructure brings together systems built for separate purposes, technologies from different eras, products from various vendors, and platforms from various services and permits them to interoperate. DIS exercises are intended to support a mixture of virtual entities (human-in-the-loop simulators), live entities (operational platforms and test and evaluation systems), and constructive entities (wargames and other automated simulations).

G.2 INFORMATION PROCESSING STANDARDS

IEEE Standard 1278 is described in both the Information Transport and the Information Modeling and Data Exchange sections of this appendix. Used together, these standards will define an interoperable simulated environment, and will specify the requirements that need to be met by simulations participating in a Distributed Interactive Simulation.

G.2.1 Mandates

There are no exceptions or extensions to this section.

G.2.2 Emerging Standards

Two recent Defense Science Board Task Forces, along with other studies, have noted the need to broaden Modeling and Simulation (M&S) architectural activities into the development of a high level architecture in order to promote greater interoperability and reuse of models and simulations and to support other functional areas such as virtual prototyping in acquisition. In response, the DOD architectural Modeling Group is developing the High Level Architecture (HLA) for broad use by development programs across a wide spectrum of DOD application domains. The HLA describes a common technical framework for the Simulation domain and is put forth as an emerging standard. The HLA is being designed to allow a combat or system developer to build HLA-compliant prototype that can be "plugged-and-played" in a rich simulated battlefield environment to evaluate system performance, limitations, and contribution to battlefield combat power, well before actual design prototypes are available.

ARPA also developed the Aggregate Level Simulation Protocol (ALSP) to interconnect theater-level constructive simulations. The resulting confederation of Service simulations (e.g., Corps Battle Simulation, Air Warfare Simulation; Research, Evaluation, and System Analysis) has been assembled and used with success to support a wide spectrum of joint and combined training exercises (e.g., Atlantic Resolve, Unified Endeavor, Ulchi Focus Lens). ALSP confederations will remain a cornerstone of joint force level training for the next few years until the Joint Simulation System reaches Initial Operating Capability.

M&S will become increasingly dependent on Object Oriented Technology (OOT). OOT emerging standards for simulation include:

1) Those contained in the Object Data Management Group (ODMG) document ODMG-93

2) The American National Standards Institute (ANSI) SQL3 (also called Object SQL)

3) The unnamed Unified Commercial Off The Shelf (COTS) standard approach being developed by the OOT industry.

The Conceptual Models of the Mission Space (CMMS) is a first abstraction of the real world and serves as a frame of reference for simulation development by capturing the features of the problem space. Those features are the entities involved in any mission and their key actions and interactions. The CMMS is a simulation neutral view of the real world and acts as a bridging function between the Warfighter, who owns the combat process and serves as the authoritative source for validating CMMS content, and simulation developers. Additionally, the CMMS provides a common viewpoint and serves a vehicle for communications among Warfighters, doctrine developers, trainers, C4I developers, analysts, and simulation developers. Such a foundation allows all concerned parties to be confident that simulations are founded in operational realism.

Standard representation of the natural environments will offer stability in the M&S RDT&E sampling requirements. Models of military operations depend on interaction with representations of natural environment including permanent and semi-permanent man-made features. Further realistic representation of military operations requires integration of weapons effects and resulting environments. This requires authoritative three-dimensional representations of the terrain, oceans, atmosphere, and space to include environmental quality issues (e.g., conservation, pollution prevention). Environmental representations must be seamless in terrain, ocean, atmosphere, and space boundary regions to fully present fully integrated data for M&S use.

G.3 INFORMATION TRANSPORT STANDARDS

IEEE 1278.2-1995: DIS Communication Services and Profiles

SCOPE: This standard establishes the requirements for the communication services to be used in a Distributed Interactive Simulation application. This standard supports IEEE 1278.1-1995. Addressing of host computers is handled by the mechanisms provided by this document and incorporated within the profiles. This document provides two such profiles for use with existing DIS applications. Later versions of this standard will specify other profiles that may be used with DIS applications. It is up to the users to determine which profile will satisfy the requirements for a particular exercise. Furthermore, this document only addresses the communication services network layers 3 and 4 of the Open Systems Interconnection (OSI) Reference Model. It is envisioned that future versions of this document will address the remaining layers (5, 6, and parts of 7).

PURPOSE: The purpose of this document is to establish requirements for communication subsystems that support Distributed Interactive Simulations. This standard provides service requirements and associated profiles that can be individually selected to meet specific DIS system operational requirements. Profile-1 and profile-2 are currently the only profiles provided. It is expected that requirements for communication services applicable to emerging DIS applications such as Field Instrumentation will be more fully addressed in a future version.

G.4 INFORMATION MODELING AND DATA EXCHANGE STANDARDS

G.4.1 IEEE 1278.1-1995: DIS Application Protocols

SCOPE: This standard defines the format and semantics of data messages, also known as Protocol Data Units (PDUs), that are exchanged between simulation applications and simulation management.

PURPOSE: The PDUs provide information concerning simulated entity states, the type of entity interactions that take place in a DIS exercise, and data for management and control of a DIS exercise. This standard also specifies the communication services to be used with each of the PDUs.

G.4.2 IEEE 1278.3-1995: DIS Exercise Management and Feedback

SCOPE: . This standard addresses the exercise control and feedback stations connected into DIS networks. IEEE Standard 1278.3, currently in revision prior to balloting recirculation, provides a recommended practice for Distributed Interactive Simulation exercise management and feedback

PURPOSE: Exercise management and feedback stations are not currently covered by standards. In fulfilling this need, the working group will define the functions that must be implemented in Exercise Management and Feedback Stations. These functions will allow the exercise manager to control exercise participants and to provide feedback of exercise results to participants; both groups distributed geographically.

The recommended practice provides procedures and guidelines used to plan, set up, execute, manage and assess a DIS exercise. It provides guidelines for sponsors, providers and supporters of DIS compliant systems and exercises. It provides functional requirements for developers of DIS exercise management and feed back stations. It specifies the functions of the organizations involved in a DIS exercise and the top level process recommended to accomplish those functions. Special attention is paid to the elements of this process that support verification, validation, and accreditation of the DIS exercise.

G.5 HUMAN-COMPUTER INTERFACES

There are no exceptions or extensions to this section.

G.6 INFORMATION SECURITY

There are no exceptions or extensions to this section.

This page was intentionally left blank.

This is the last page.

Filename:	ATA01306.DOC
Directory:	C:\RMELTON
Template:	C:\WINWORD\TEMPLATE\NORMAL.DOT
Title:	MDA WP First Half
Subject:	
Author:	SAIS
Keywords:	
Comments:	
Creation Date:	02/01/96 3:57 PM
Revision Number:	16
Last Saved On:	02/05/96 2:51 PM
Last Saved By:	LTC William A. Teter
Total Editing Time:	243 Minutes
Last Printed On:	10/04/96 10:12 AM
As of Last Complete Printing	
Number of Pages:	113
Number of Words:	31,362 (approx.)
Number of Characters:	178,765 (approx.)